A SPECIAL FEATURE SECTION

Security For The Internet of Things
Get to Market Faster and More Profitably

From solution design and development through deployment and support, Avnet is uniquely equipped to help you get your solution to market faster and more profitably – anywhere in the world.

If you are looking for ways to expand the market opportunity for your technology solution, look to Avnet. With our deep technical expertise, global footprint and relationships with leading hardware manufacturers we can take unnecessary time, cost and complexity out of your business so you can focus on what you do best. We also have experience in software-defined, converged and hyper-converged systems which can be integrated and optimized for the needs of your solution.

Put your technology solution on the fast track. Go to [www.em.avnet.com/appliancesolutions](http://www.em.avnet.com/appliancesolutions) to learn more about Avnet's Integrated Systems and Appliances.

Contact us for more information at appliancesolutions@avnet.com.
SPECIAL SECTION
SECURITY FOR THE INTERNET OF THINGS

14 Security for the Internet of Things—Let’s Begin the Conversation
by Tom Williams, Editor-in-Chief

How PRPL id Addressing Security Requirements
by Kathy Giori, Qualcomm

Embedded Hardware & Software Partnerships Provide Critical Path to Closing IoT Security Loopholes
by Jeff Sharpe, ADLINK Technology

IoT Security – A Holistic Approach
by Robert Andres, Eurotech

OT and IT Coexist in a Secure IIoT World
by Exara

In IoT Security, We Trust
by Gregory Rudy, Green Hills Software

Basic Security Techniques Really Work
by Alan Grau, Icon Labs

How to Secure IoT Through the Home Gateway
by Andy Weitzner, Ikanos Communications

Securing SoCs in the IoT Era
by Kevin McDermott, Imagination Technologies

prpl is Pragmatic for Security
by Simon Davidmann, Imperas Software

Solving IoT Security Problems with New Generation of FPGAs
by Kevin McDermott, Imagination Technologies

TECHNOLOGY CORE
ARM: REACHING FROM SENSOR TO SERVER

30 Embracing ARM in the Cloud Datacenter
by Karl Freund and Dilip Ramachandran, AMD

TECHNOLOGY CONNECTED
MAINTAINING SECURITY FOR WIRELESS CONNECTIVITY

34 Securing Consumable Components in an Embedded System Design
by Robert Van Rooyen, Barr Group

TECHNOLOGY IN SYSTEMS
HYPERVERSORS AND VIRTUALIZATION

38 Multicore Performance Requires NUMA-Aware Hypervisor Design
by Timo Kuehn and Raphael Baum, Real-Time Systems

42 What Software Strategy Makes Best Use of Multicore Processors?
by Robert Day, Lynx Software Technologies
When the success of your mission is on the line, you can’t afford to waste time and money on poor technical support or products with long lead times. With over 30 years of being a key supplier to the MIL/COTS industry, WinSystems understands your needs of products that withstand harsh environments, continuous uptime and long term availability. Our engineers are ready to guide you through product selection, customization, implementation and lifelong support.

Considered by our clients, to be The Embedded Systems Authority, WinSystems focuses on the latest rugged embedded technology and provides a consultative approach to your systems design.
What is a disruptive technology? A disruptive technology is one that displaces an established technology and shakes up an industry, market or value network over a fairly short time, or it can be a ground-breaking product that creates a completely new industry. We have seen a good many—the PC, the cell phone, smartphone, email—the list goes on. Right now we appear to be perched on the edge of a disruption brought about by the convergence of several technologies: electric vehicles, solar/wind power, advances in battery and storage technology and the Smart Grid enabled by industrial Internet technology.

All of these, of course, have one thing in common—they are enabled by embedded computer intelligence. They are also achieving advances, some under the public radar, that are making them more efficient and more cost effective. And their growing synergy is moving us toward a future that is powered by renewable sources for both general electrical consumption and transportation and will move us away from fossil fuels simply by consumer choice and economics, not as a result of government regulation.

Take solar, which is of course based on silicon technology but new research is taking it into other materials such as thin film technology that uses narrow coatings of cadmium telluride and other means to increase efficiency. In addition, low-cost, powerful microcontrollers are making it possible to place DC/DC and DC/AC converter controllers on each solar panel greatly improving output and preventing one failing or shaded panel from bringing down the output of the whole array. Recently, researchers at Ohio State developed a battery that is some 25% less expensive than other designs and can be integrated into each panel along with the electronics. Manufacturing improvements have recently made possible back contact designs, which allow more surface area to be used for energy collection.

Improvements in storage technology are essential to renewable energy sources for times when the sun isn’t shining or the wind dies down. On-panel batteries as well as larger and more efficient batteries are fueling a debate over whether solar power can or will go mostly off-grid, share power production and storage over the Smart Grid or be based largely on central production facilities. The latter now seems the least likely and traditional utilities are very definitely in the path of this disruptive technology. The Smart Grid is being looked at for use as more local microgrids that can distribute power among users with different needs and capacities as well as manage storage and manage demand response operations for times of high demand.

All of this will and does rely on embedded technology so whichever way it goes, the future looks bright for the embedded industry.

And then there are electric vehicles that for some time have been curiosities or the target of amused ridicule. Like many disruptive technologies before them, EVs may lurk a while longer on the sidelines before they go mainstream and heavily affect the oil industry. Talk about disruption . A recent issue of Consumer Reports rated the new Tesla Model S P85D at a score of 103 breaking its own rating system, which had a top score of 100. It wasn’t claiming it was a perfect car—there were still some issues of interior materials and cup holders. And it certainly wasn’t presenting the $127,820 vehicle as the ideal family car, but as a signpost to the future.

We have all seen how initially expensive technologies can drop radically in cost as the volume grows, the basics are refined and features improved—and, of course, when competition ensues. Tesla is is ramping up production and preparing two new models including the Model X crossover in 2016 and the Model 3 compact sedan in 2018. The latter is expected to be priced at around $35,000. You can bet other manufacturers are not sitting on their hands in the face of this. And I hardly need point out that like all modern automobiles, EVs are chock full of electronics and mountains of software.

Tesla is also investing over a billion dollars building a battery factory in Nevada. It is expected to produce advanced batteries for both vehicles and for energy storage for home rooftop solar systems. And, of course, this is just the beginning. Networks of charging and battery-swap stations are starting to appear just like gas stations did at the start of the automotive age. Further out, there is development going on for roadways that have a clear surface covering solar collectors and a channel down the middle for optical Internet lines. There are ideas for transferring energy directly from such roadways to vehicles moving over them.

Connectivity is naturally key to all this. Data and control moving over microgrids within the Smart Grid, to balance loads, share power produced and keep track of users’ credits and debits, demand response and activation of storage systems—all build on what now is merely the foundation of the Internet of Things. Wireless communication among vehicles, with the roadway and beyond both for control, navigation, automatic driving, infotainment and more. There will be casualties and winners as the process advances, but it looks like it is gaining the critical momentum that won’t be stopped.
INDUSTRY INSIDER

New Weightless 2-Way Communication IoT Standard Launches

The Weightless SIG has announced the deployment of Weightless-N Smart City networks from Nwave Technologies across Copenhagen. The Weightless SIG has announced that M²Communication (M2COMM), a leading provider of industrial IoT connectivity technologies, has joined the Weightless SIG to lead a Weightless Working Group for the development of a new high-performance LPWAN standard. This latest standard, called Weightless-P, will offer uplink and downlink capabilities to significantly enhance quality of service especially important in the very stringent industrial IoT sector.

Adapted from field-proven experiences, Weightless-P supports all major license-exempt SRD/ISM bands including 169, 433, 470 - 510, 780, 868, 915 and 923MHz, ensuring worldwide availability. The standard provides fully acknowledged 2-way communication offering best-in-class quality of service at data rates ranging from 200bps to 100kbps. It enables higher capacity than existing LPWAN and cellular technologies for uplink-dominated traffic with short-to-medium payload sizes. Using common commercially-available chipsets, it will also support both stationary and mobile end devices by utilizing low-power, innovative handover, cell re-selection and roaming methods. Other advanced reliability features include fast network acquisition, paging, FEC, ARQ, power control and adaptive channel coding.

The range and reliability, from challenging dense urban to rural environments, will exceed alternative LPWAN technologies using up to 17dBm output power.

The Weightless-P specification is expected to be published and available to SIG members in Q4 2015. Weightless-P hardware, including development kits, is expected to be launched early in 2016.

VITA Standards Organization Ratifies ANSI/VITA 46.11 System Management on VPX

The VMEbus Industry Trade Association (VITA) has announced that VITA 46.11 “System Management on VPX” has reached ANSI recognition as ANSI/VITA 46.11-2015. This specification has completed the VITA and ANSI processes reaching full recognition under guidance of the VITA Standards Organization (VSO).

ANSI/VITA 46.11 defines a framework for System Management in VPX systems. It enables interoperability within the VPX ecosystem at the field replaceable unit (FRU), chassis, and system levels. The framework is based on the Intelligent Platform Management Interface (IPMI) specification and leverages many concepts and definitions from the AdvancedTCA (ATCA) specification by PICMG.

“As the complexity of embedded computing systems continues to increase, so do the demands to be able to maintain these systems in a cost-effective manner,” said Daniel Toohey, Technical Director at Mercury Systems and VITA 46.11 Working Group Chair. “The task of configuring, optimizing, securing, repairing and monitoring such systems, especially when the systems are comprised of elements from various vendors can be extremely costly, technically challenging, and in some cases impossible to accomplish at all. This drove the need for consistent management interfaces, and was the genesis of VITA 46.11.”

VITA 46.11 took on the challenge of defining a set of physical, logical, and protocol requirements to standardize the management of VITA 46 and VITA 65 compliant modules and backplanes. ANSI/VITA 46.11 provides a true solution for systems management interoperability across various hardware and software vendors, chassis suppliers, systems integrators, and end users. It provides consistent management capabilities and behaviors for these disparate elements, and provides a robust framework that allows individual implementers to add their own enhancements without impacting interoperability. Copies of the specification are available for purchase at the VITA Online Shop (http://shop.vita.com/).

Microchip Completes the Acquisition of Micrel

Microchip Technology has announced that Microchip has completed its previously announced acquisition of Micrel. Shareholders of Micrel overwhelmingly approved the merger with 98.95% of the Micrel shares that voted in favor. As a result of the completion of the transaction, trading in Micrel common stock on the NASDAQ Stock Market has ceased.

Under the terms of the merger agreement, Micrel shareholders were able to elect to receive the $14.00 per share purchase price in either cash or shares of Microchip common stock. Based on the results of the shareholder elections, Microchip will pay an aggregate of approximately $430 million in cash and issue an aggregate of 8,626,795 shares of its common stock to Micrel shareholders. The number of shares of Microchip common stock that a Micrel shareholder will receive is based on a conversion ratio of $14.00 divided by the average of the Microchip closing stock price for the ten most recent trading days ending on the second to last trading day prior to August 3, 2015, which is $42.888 per share.
Pentair announces the acquisition of Pigeon Point Systems, a producer of high-quality management components, focusing on open modular platforms such as AdvancedTCA, MicroTCA, CompactPCI and VPX. By combining Pigeon Point Systems products with Pentair’s broad range of Schropp products, Pentair will be able to provide an expanded product portfolio, increase presence globally and provide broader technical expertise to serve Pentair customers and their ever increasing needs in embedded computing and reliable system monitoring and control.

“This acquisition expands our position in monitoring and control,” said Volker Haag, VP Global Systems Category and Innovation, Pentair Electronics Protection. “It provides Pentair with several new dynamic product lines for growth and complements Schropp branded chassis and systems.”

Pigeon Point Systems focuses on providing dependable, proven solutions for management controllers and allows customers to concentrate on the value-add aspects of their products. Their deep expertise in open standards ensures compliance and interoperability for their components based on those standards.

Pentair is a leader in providing safe and reliable products designed to protect electronic boards, represented by its well-known Schropp brand. It is well recognized for systems targeting embedded computing like those based on the AdvancedTCA, MicroTCA and CompactPCI standards and has a great history in subracks, cases, cabinets and PCB accessories as well as cooling and power supplies.

Pentair Acquires Pigeon Point Systems to Expand its Schroff Portfolio for Monitoring Systems

Pentair announces the acquisition of Pigeon Point Systems, a producer of high-quality management components, focusing on open modular platforms such as AdvancedTCA, MicroTCA, CompactPCI and VPX. By combining Pigeon Point Systems products with Pentair’s broad range of Schropp products, Pentair will be able to provide an expanded product portfolio, increase presence globally and provide broader technical expertise to serve Pentair customers and their ever increasing needs in embedded computing and reliable system monitoring and control.

Pigeon Point Systems focuses on providing dependable, proven solutions for management controllers and allows customers to concentrate on the value-add aspects of their products. Their deep expertise in open standards ensures compliance and interoperability for their components based on those standards.

Pentair is a leader in providing safe and reliable products designed to protect electronic boards, represented by its well-known Schropp brand. It is well recognized for systems targeting embedded computing like those based on the AdvancedTCA, MicroTCA and CompactPCI standards and has a great history in subracks, cases, cabinets and PCB accessories as well as cooling and power supplies.

Low-Voltage Motor Suppliers Unsure of Impact of Energy Efficiency Regulations

It is widely accepted that integral horsepower low-voltage (LV) motors make up an estimated 28% of annual global electric energy consumption. However, with an increasing number of motors set to undergo stricter energy efficiency regulations by 2017, this percentage is likely to decline. Even a 1% efficiency gain for a low-voltage motor can save thousands of dollars in electricity costs over the lifetime of a motor, according to the recently released report “The World Market for Low-voltage Motors” by IHS Inc. (NYSE:IHS). With varying energy efficiency legislation in different regions around the world, it is very important to track the success of this initiative to sell more energy-saving motors. With so many conflicting signs in the current economic environment, motor suppliers are reportedly uncertain as to how effective the recent and impending energy efficiency requirements will be.

The global motor market is highly fragmented and very mature, so change often occurs slowly. However, certain sectors react quite differently to innovation than others. An example of this can be seen within the pump, fan and compressor markets, which account for more than 2/3 of motor applications annually. Because of their usual continuous-duty requirements, motor control devices such as variable frequency drives (VFDs) and higher-efficiency IE4/NEMA Super Premium class motors are more common than in other motor applications. Because of its heavy use of these products, the HVAC industry will experience the fastest penetration rate of higher-efficiency equipment, whereas the slower-growing heavy industries, such as power generation, metal processing and mining, will be less quick to adopt newer technologies.

The key trend discovered in this report is that motor suppliers are venturing into other product categories and offerings in order to remain competitive. As further motor efficiency improvements are both expensive and, in some cases, excessive, it is logical to offer VFDs and even pumps, fans or compressors with above-average efficiency. This shift is identified as an increased focus on systems efficiency, which provides end users with more options and also allows motor suppliers to better understand their customers’ needs. The wrong equipment is purchased too frequently because the end user does not have the means to determine the proper equipment requirements for their applications. Motor suppliers now have an opportunity to train their customers and ensure that the right-sized equipment is utilized in the appropriate environment.
Green Hills Software and Luxoft Partner on Automotive HMI Design Tool Chain

Green Hills Software and Luxoft Holding have announced the integration of Green Hills Software’s INTEGRITY real-time operating system (RTOS) with Luxoft’s Populus Suite HMI design tool chain. With the use of Green Hills Software’s MULTI integrated development tool chain, this combination allows Populus to run on a wide range of automotive grade microcontrollers (MCUs), enabling the creation of robust digital instrument clusters with a low memory footprint.

Luxoft’s Populus is specially designed for operation using a low memory footprint. By addressing the specific features of the MCU, a highly optimized Populus runtime engine enables the combination of a high performance HMI with very low memory consumption for both the engine stored in the flash memory as well as the RAM memory needed during the runtime. Luxoft’s Populus Suite enables the rapid HMI development for customizable, 2D or 3D, fully digital instrument clusters, head-up displays (HUD), in-vehicle infotainment systems and entry level to mid-tier Head Units.

Security is achieved by the use of hardware memory protection to isolate and protect embedded applications. Secure partitions guarantee each task the resources it needs to run correctly and fully protect the operating system and user tasks from errant and malicious code, including denial-of-service attacks, worms, and Trojan horses.

The MULTI integrated development environment leverages 30 years of embedded software development expertise to provide developers an integrated package of tools they can trust to create reliable software efficiently. The MULTI IDE offers integrated multicore development, debugging and programming tools, including AUTOSAR operating system awareness, flash programming for on-chip flash, performance profiler, project builder, code coverage, run-time error checking, MISRA C adherence wizard, and the DoubleCheck integrated static code analyzer. The combined solution is available today.

Violin Memory’s “Disk Is Dead” Campaign Pushes the Move to Primary Storage Flash

The Grateful Dead may have performed their last live concert in Silicon Valley, but Violin Memory is raising eyebrows with its “Disk is Dead” campaign – a lighthearted but poignant tribute to the enterprise hard disk drive whose days are numbered with the rapid rise of the all flash data center.

1,000 IT professionals and contest participants were rewarded for engaging with thought leadership pieces that brought to life the data protection, performance, and cost advantages of flash. Contestants were given the opportunity to win a variety of Disk is Dead prizes, including grand prize winners who received free trips to see the Grateful Dead at the “Fare Thee Well: Celebrating 50 Years of Grateful Dead” concert at Levi’s Stadium in Santa Clara.

The first phase of Violin’s integrated “Disk is Dead” campaign fueled a dialogue among data center professionals that not only is there a better storage medium – flash – but that there are also better architectural approaches to 24x7 data center-scale storage than simply swapping one type of drive for another. The campaign showcased Violin’s Flash Storage Platform (FSP) - the ultimate enterprise storage solution for the consolidation and simplification of next generation data center workloads delivering continuous data protection with the highest performance storage at the lowest CAPEX and OPEX possible today. You can learn more about the campaign by referring to Violin’s “Bring Out Your Dead” blog, by visiting Violin’s Disk Is Dead campaign site.
Intel Conference Points to the Expansion of the IoT into Everyday Life

New technologies are enabling new ideas for expanding pervasive computing power into all walks of life—work, health, recreation and social interaction. The Internet of Things appears poised to embrace most of our daily activities.

by Tom Williams, Editor-in-Chief

The recent Intel Developers Forum (IDF) held in San Francisco has shed light on Intel’s direction for the coming year as well as some new technology developments. As embedded computing inexorably spreads out of the industrial/military realm and into the world of everyday consumers, huge opportunities are opening up along with the need to adapt the technology to the conditions of a mobile, wearable world in which the users may have no idea of the underlying technology but expect it to function flawlessly and intuitively to meet their needs and expectations.

To that end, Intel has announced a number of technology advances as well as directions for development based on those technologies. One thing that has come to be expected at each IDF is the next iteration of Intel’s foundation Core processor technology in its yearly “tick” (advance in process technology) “tock” (advance in microarchitecture) model. This is the year for the “tock,” which while not quite ready, heralds advances in a Core-based multicore SoC code named “Skylake,” which will bring enhanced instructions, more integrated IP including advanced on-chip graphics and perhaps most urgent, lower power consumption now that Intel is in a cosmic struggle with ARM on all levels including the 64-bit server market. But that’s another topic.

Making Systems Intuitively Interactive

One area directly aimed at consumers but with major implications elsewhere is Intel’s RealSense technology. In collaboration with Google, Intel is driving innovation in mobile depth sensing by implementing Intel RealSense technologies into an Android Smartphone developer kit that was demonstrated at IDF. The Intel RealSense Smartphone featuring Google’s Project Tango enables new experiences including indoor navigation and area learning, virtual reality gaming, 3D scanning and more. Intel RealSense developer kits supporting Project Tango are targeted to reach select Android developers by the end of this year.

One key to the RealSense effort is the use of 3D cameras that use depth-sensing technology and a camera interface that can give developers access to a camera’s raw depth data. This enables a number of application areas such as gesture and face/facial expression recognition. Users will soon be able to scan 3D objects and from the scans create 3D models within the computer. A major application area will be robot vision. One application demonstrated was a Robot Butler built by Savioke now being used by some hotel chains to deliver items like room service requests, etc., to rooms. The butler can autonomously navigate the path, avoiding objects and persons along the way. And you don’t have to tip it. Of course, gaming will also be a big market for RealSense, which is already available on some new PCs, and development kits are available as well.

Another result that is under development in the RealSense arena is a pseudo-holographic display that projects a 3D image in proximity to the terminal. The display will be manipulated...
by touch and provide what is called haptic feedback. This is the generation of tactile sensation, vibrations, that can give the user a more real sense of interaction with the display. It, of course, also reacts to the presence and movement of a hand or finger interacting with the 3D display.

**Pushing for Security**

Intel's Enhanced Privacy ID technology has been deployed for something like five years. But Intel is now announcing major partnerships with both Atmel and Microchip Technology incorporating it into their own products. The EPID technology delivers a hardware root of trust. With Intel EPID, devices can be identified and a secure communication can be linked between these devices. Additionally, the group membership can be determined without revealing the identity of the specific platform allowing for another level of security. Intel EPID can dynamically assign and revoke group memberships by individuals. Even more, this technology meets the latest protected key delivery requirements for content and data protection protocols.

One interesting demonstration showed a user accessing a device. The user was wearing a bracelet with an RF link to the device and a specific code in the bracelet. When the user entered the correct password, it was matched with the worn ID code and access was granted. If the user went out of range of the device or disconnected or removed the bracelet, it would require the reentry of the password to match the code. The assumption here is that only that user knows the password that goes with his/her ID. Other scenarios are of course possible.

**Memory Breakthrough**

With CPU speeds now far outpacing what most RAMs are capable of, a new announcement by Intel and Micron Technology introduced a new class of nonvolatile memory that is 1,000 times faster than NAND flash and 10 times denser than conventional memory. An individual die can store up to 128 Gbits of data. Called 3D Xpoint, the new technology is the result of more than a decade of research and development. 3D XPoint was built from the ground up to address the need for non-volatile, high-performance, high-endurance and high-capacity storage and memory at an affordable cost. It ushers in a new class of non-volatile memory that significantly reduces latencies, allowing much more data to be stored close to the processor and accessed at speeds previously impossible for non-volatile storage.

The new, transistor-less cross point architecture creates a three-dimensional checkerboard where memory cells sit at the intersection of word lines and bit lines, allowing the cells to be addressed individually (Figure 2). As a result, data can be written and read in small sizes, leading to faster and more efficient read/write processes.

Intel also introduced its new Optane technology, which is based on the 3D XPoint non-volatile memory media and combined with the company’s advanced system memory controller, interface hardware and software IP, to unleash vast performance potential in a range of forthcoming products. Intel Optane technology will first come to market in a new line of high-endurance, high-performance Intel SSDs beginning in 2016. The new class of memory technology will also power a new line of Intel DIMMs designed for Intel’s next-generation data center platforms. It could logically be expected that such a breakthrough will lead to a wide variety of implementation, many of which could vastly increase the power and performance of small devices.

**The World of the Wearable**

As the IoT permeates our lives, the push for ever smaller, unobtrusive and wearable systems is accelerating. Intel’s response is the Curie SoC that was first announced in January and is now sampling with shipping expected later in 2015. The Curie is based on Intel’s 32-bit low-power Quark microcontroller. It incorporates Bluetooth low energy, a low-power integrated DSP sensor hub and pattern matching technology along with a 6-axis combo sensor with accelerometer and gyroscope. These elements combine to make up a pattern classification engine that allows it to identify different motions and activities quickly and accurately. In addition it has on-chip 384 kBytes of flash and 80 kBytes of SRAM plus battery charging circuitry. The module is packaged into a very small button-sized form factor and runs a new software platform created specifically for Intel Curie module.

Intel also announced plans to create multiple reference designs based on the module that will be available through select ODMs. As example, Intel demonstrated the first reference design for enterprise wearables, which features enterprise grade security and consumer grade usability. The device allows the wearer to authenticate once on a phone or a PC and carry that authentication with them, enabling automatic login when in close proximity.
Intel also announced a new end-to-end software platform created specifically for the Curie. The platform includes all of the hardware, firmware, software, SDK and services needed for a variety of use cases. The software platform supports iOS and Android devices and allows manufacturers to create their own unique and differentiated products.

Newly announced at IDF are two new Intel IQ Software Kits—Intel Identity IQ and Intel Time IQ, which will be released by the end of 2015. The kits include Identity IQ, which establishes the identity of the user of the wearable device and enables personalized and secure experiences with services that require personal authentication. The Time IQ aims to improve the efficiency of wearable users’ daily routines and accomplish tasks with contextually-aware notifications.

ABody IQ enables capabilities related to physical activities, including counting steps and calculating calories burned as well as providing data visualizations to help achieve goals. And finally, a Social IQ supports social interactions, including communication via phone, social networks and SMS with peers and brands.

This year’s Intel Development Forum brought together Intel’s new technologies and exposed them to a growing number of developers and OEMs that are increasingly devising applications that affect users’ daily lives. The emphasis on usability and the awareness of the spread of the IoT into not only industry, but also medicine, health, design, and social interaction was quite apparent and can be expected to result in some very compelling products and applications in the near future.

**Intel, Santa Clara, CA**
(408) 765-8080. www.intel.com

**Atmel, San Jose, CA**
(408) 441-0311. www.atmel.com

**Microchip Technology, Chandler, AZ**
(480) 792-7200. www.microchip.com

**Micron Technology, Longmont, CO**
(720) 494-5000. www.micron.com

**Savioke, Santa Clara, CA**
www.savioke.com
Embedded/IoT Solutions

Connecting the Intelligent World from Devices to the Cloud
Long Life Cycle • High-Efficiency • Compact Form Factor • High Performance • Global Services • IoT

IoT Gateway Solutions
Compact Embedded Server Appliance
Network, Security Appliances
High Performance / IPC Solution

Cold Storage
4U Top-Loading 60-Bay Server and 90-Bay Dual Expander JBODs

SYS-5018A-AR12L
SYS-5028A-TN4
SYS-5018A-FTN4 (Front I/O)
SYS-6018R-TD (Rear I/O)

2015 COMPUTEX Taipei
JUNE 2-6TH, 2015
Come visit our booth @ 4th Floor M0120

• Standard Form Factor and High Performance Motherboards
• Optimized Short-Depth Industrial Rackmount Platforms
• Energy Efficient Titanium - Gold Level Power Supplies
• Fully Optimized SuperServers Ready to Deploy Solutions
• Remote Management by IPMI or Intel® AMT
• Worldwide Service with Extended Product Life Cycle Support
• Low Power Intel® Avoton, Rangeley, Quark, Core™ i7/i5/i3 and High Performance Intel® Xeon® Processors E3-1200 v3 product family
• Optimized for Embedded Applications

Contact us at www.supermicro.com/embedded

© Super Micro Computer, Inc. Specifications subject to change without notice. Intel, the Intel logo, Intel Inside, and Xeon Inside are trademarks or registered trademarks of Intel Corporation in the U.S. and/or other countries. All other brands and names are the property of their respective owners.
Security for the Internet of Things—Let’s Begin the Conversation

by Tom Williams, Editor-in-Chief

Computer security has been a never-ending struggle over many years. The importance and urgency of security increases with the spread of technology and our dependence on it, with its ever-growing realm of applications and the more accessible it becomes to the general public. And with that, really implementing security becomes increasingly complex, multifaceted and just plain difficult. Long-time readers of RTC may recall that I have occasionally expressed skepticism regarding claims of security as well as the ability to totally achieve it. Despite any misgivings, however, security is necessary and imperative if the Internet and now the Internet of Things are to become viable technologies and a viable market. As they increasingly become a part of all our daily lives, our dependency on them becomes a matter of personal, economic and social well-being. As a result, we are witnessing an intense increase in research, innovation and implementation of security measures at all levels—from sensor and device to the Cloud.

The rise of the IoT has multiplied the issues and levels and strategies devoted to security perhaps due to a bit of an internal paradox. While on the one hand, we want everything to be connected in the abstract sense, i.e., potentially for any user or node to be able to connect to any other, we don’t really want that. We want selective and protected access. We want private or restricted domains within this world-spanning ibernetwork. We want a straightforward way to grant or deny access to specific users, to select levels of access to those admitted, yet we also want to be able so search for those resources that are available for our purposes. And we want adequate security to protect the functionality of small, hardware-restricted sensors and actuators as well as gateways and edge devices. We want the data in transit to be secure and yet have it selectively accessible to other authorized users. It’s a very tall order but one that is vitally necessary. And that is why we want to start a conversation.

You will find in this special section on IoT Security a selection of short position papers and points of view from a number of leading companies. They exhibit both a diversity of approaches as well as many areas of agreement on the scope and the needs for a continuum of security. We present this section to give our readers a feel for the number of companies that are active in this area—and there are many more. We also hope that this collection of relatively brief statements will lead to an ongoing technical conversation in the form of contributed articles and opinion pieces that we will carry in the pages of RTC throughout the coming year. We are changing our previous section that was titled, Technology Connected to the name Technology and the Internet of Things. There are certainly many more aspects concerning the IoT than security alone and we will definitely be carrying articles on those many topics as well. But we hope to include at least one piece dealing with security issues in each month’s section.

So consider this to be both an introduction as well as an invitation to take part in an energetic and compelling conversation both as colleagues as well as competitors. It is our hope that through such an exchange we can all gain and confidently continue to build what is shaping up to be a major technological development for the entire world.
How PRPL is Addressing Security Requirements

by Kathy Giomi, Qualcomm

When it comes to digital security, the world takes the matter seriously, and who wouldn’t? In today’s always connected world, data from our pocket phones reaches out and back to the Internet frequently. We want to ensure that our information is protected no matter where we are and what other Wi-Fi access points (APs) we connect through as an on-ramp to the Internet. Does an AP built from open source software mean that the data it carries is less secure? No.

Openness has been shown to improve platform security. With open source software, vulnerabilities can be fixed much faster. Anyone in the world can write, test and apply a patch, and share that fix with others. If the source to create a patch is not available, then there will be a bottleneck to obtaining a fix. In such cases of limited or no access to original source, it may not be possible to obtain a patch to block an exploit. The consumer would be left vulnerable.

On the other hand, when regulatory bodies impose operational limitations on platforms, maintaining that compliance may require a different form of security – closed or limited access to source. For example, there is a restriction placed by the Federal Communications Commission (FCC) on Wi-Fi AP operation that is intended to protect Doppler weather radar operation at airports. Accurate readings of weather radar are important for air-traffic controllers to warn pilots who are flying near that airport and safely route them around dangerous storms. Given access to open source software that includes logic to control regulatory restrictions, an intelligent Linux developer would be capable of negligence in terms of disabling FCC protections on an AP.

We need openness for improved security, but openness leaves an opportunity for abuse of regulatory compliance. The question becomes, how do we satisfy these opposing constraints?

Such challenges are being tackled by members of the prpl Foundation, an open source non-profit focused on enabling next-generation datacenter-to-device portable software and virtualized architectures. In particular, there are two prpl Engineering Groups (PEGs) working on this dilemma: one focused on improving OpenWrt (a popular embedded Linux distribution), and the other focused on improved security in general.

When software is open, some means need to be put in place to ensure that modifications to the software can’t easily break compliance. Two methods to address this problem are being tackled. The first is a purely software-based approach. Software packages are compiled as binaries before being loaded on a platform. The images can be securely “signed” by a trusted source. Linux already allows for checking the validity of the signature of the regulatory database, which can only be signed by the regulatory database maintainers. The trick of this approach is making sure all vendors and after-market software distributions such as OpenWrt comply by keeping the signature checking in place. This honor system approach can ensure compliance of mass marketed binary images, leaving the gap of regulatory abuse quite limited due to the extreme expertise needed to break the rules.

Another approach takes advantage of new hardware virtualization capabilities. With this approach, a limited slice of hardware and software functionality that handles regulatory compliance is isolated from the openness and flexibility afforded by the rest of the platform. Again, access to changes within the narrow regulatory compliance slice would be highly restricted. But access to innovate and apply security patches to everything else would be maintained far more openly and flexibly.

By working alongside companies like Qualcomm Atheros, prpl Foundation hopes to highlight the importance of openness for innovation and security purposes and strives to find common ground with the FCC on these particular issues.

Qualcomm
San Diego, CA
(858) 587-1121
www.qualcomm.com

prpl Foundation
www.prplfoundation.org
With a seemingly countless number of connected devices, the Internet of Things (IoT) is growing steadily and rapidly. Organizations are working diligently to quickly take advantage of what IoT technology can do. In order to do so, they need solutions that are affordable, reliable, and pre-validated. Computer-on-Modules are a key component to creating IoT solutions that meet these requirements and significantly reduce time-to-market for the OEM.

congatec has paired its Computer-on-Modules with the Intel® Gateway Solutions for IoT software package from Intel®, Wind River and McAfee. This pairing can be found in congatec’s Qseven IoT kit - conga-QKIT/IOT. The IoT kit provides a pre-integrated and open platform starter kit to bring secure IoT solutions quickly to market. The Qseven IoT kit contains a Qseven Computer-on-Module (COM) based on the latest Intel Atom processor technology, a compact IoT carrier board, a 7” LVDS single touch display with LED backlight, and an extensive set of accessories including AC power supply and 802.11 WLAN antenna with IoT Wind River Linux image on a USB stick. With this kit, developing an IoT demo system takes a matter of minutes.
conga-QKIT/IoT
Qseven IoT Gateway Development Kit

~ conga-QA3 Intel® Atom™ Processor-Based Qseven Module
~ Full featured Qseven IoT Mini Carrier Board
~ 7” Single Touch Display With Cable Set
~ Intel® Dual Band Wireless-AC 7260 Card & Antenna
~ Power Supply 5V/4A, 20W, 4pin Jack
~ Intel® IoT Gateway Solution OS (Wind River IDP trial)

Find more details at: www.congatec.us
congatec Inc. | 6262 Ferris Square | San Diego CA 92121
Phone: 858-457-2600 | sales-us@congatec.com
Embedded Hardware & Software Partnerships Provide Critical Path to Closing IoT Security Loopholes

by Jeff Sharpe, ADLINK Technology

It is estimated that there could be between 25-50 billion connected devices by 2020, with more than six connected devices per person. The technologies that make up the Internet of Things (IoT) include sensors/actuators, wireless communications, hardware/software, network infrastructure, addressing and cloud computing. As these IoT technologies continue to rise exponentially, so do the security risks of breaches and unwanted data capture.

Imagine an IoT device regulating insulin injections being taken over and controlled by a hacker. This attack could easily cause major bodily injury, or even death. The IoT is dramatically increasing the vulnerabilities of environments that – when previously unconnected – did not pose the same kind of risk. This makes it increasingly important for those developing IoT solutions to work within their hardware/software partner ecosystems to address security risks at every level of IoT system design, deployment and on-going function.

In a recent survey done by the SANS Institute, the five greatest threats to the IoT over the next five years will be:

- Weakening perimeters - Difficulty patching, leaving systems vulnerable (31%)
- Botnets/malware - Things used as infection vectors to spread to enterprise (26%)
- Denial of Service (DDOS) - Attacks causing damage or loss of life (13%)
- Data breaches - Intended sabotage and destruction of device(s) (12%)
- Inadvertent breaches - User error/accidental data breaches / exposures (11%)

All of these attacks are based on the various layers implemented on the network such as Physical Layer (Eavesdropping), Data Link Layer (Spoofing), Network Layer (Wormhole), Transport (Flooding) and Application (Modification).

Current network security, internet encryption, and typical PC-based security software is not sufficient enough to protect users, data and IoT devices. There have been countermeasures proposed to address the security concerns, but we have a long way to go to bridge the gap.

The IoT industry is implementing key elements to reduce specific network security threats. Devices, gateways, servers and network routing gear must have the ability to actively reduce key security areas for encryption and breach protection, while ensuring privacy rights, ease-of-use and the ability to autonomously upgrade and provide new security patches.

A positive trend has been the development of partner eco-systems between embedded hardware and software providers to reduce the risk of IoT attacks and breaches in IoT devices and gateways. Offering boot up and memory protection at the processor level, packet encryption solutions, hardware monitoring and threat detection services, analytics of key patterns and user behaviors, and the reporting and logging of specific threats are just some of the ways that solution providers are addressing the IoT security infrastructure.

An example of a secure environment created by a partner eco-system is ADLINK’s SEMA Cloud platform, which incorporates a security framework using many of the aforementioned tactics. At the board level, Secure Boot provides a mechanism to prevent loading of unauthorized software during device boot up. For operating system security, McAfee Application Control provides whitelisting to guard against software tampering and malware zero-day exploits. Transport Layer Security (TLS 1.2) ensures secure, reliable data transfer from the device to the cloud through state-of-the-art encrypted data transmission protocols (e.g., Advanced Encryption Standard AES-256). And in the cloud, ADLINK works with leading global platform hosting partners to provide an ultra-secure environment. Finally, authentication processes using application and device specific keys are offered throughout the course of data transfer.

With the experience of early IoT market engagements, vendors can better visualize and reduce threats before they happen in order to offer customer solutions that de-risk and countermeasure security threats. The key is working together with our partners at every level of solution development to create secure IoT environments and move the conversation away from the negative outcomes of the IoT and back to all of the positive improvements that come from a connected world.

ADLINK Technology
San Jose, CA
(408) 360-0200
www.adlinktech.com
IoT Security – A Holistic Approach

by Robert Andres, Eurotech

I suspect many Internet of Things solution providers have a goal similar to ours – to maintain customer trust and confidence by ensuring the integrity, availability and confidentiality of customer data. IoT solutions are complex, with many possible points of failure and any company can be the target of a security breach.

Customers are often looking for a “security solution” or vendors who have “secure solutions.” However, there is no single solution since it is essential to look at the entire system holistically and address security at each potential point of failure. As shown in Figure 1, security can fail at any point from the sensors to the cloud to the business application.

In order to safely address all possible points of failure, security must be a fundamental part of the overall architecture of an IoT system. IoT system architects must account for the specific challenges of distributed, unattended, mobile devices and implement security both end-to-end and in each individual element.

Consider the following best practices to ensure complete IoT system security:

• Build solutions based on open and industry standards
• Leverage proven IT/enterprise class security technologies
• Include security, scalability and resiliency in design from day one
• Encapsulate the complexity of an end-to-end security solution
• Continuously test and audit the system

Device and service authentication: The IoT requires remote sensors, actuators, and smart devices to be integrated with business and mobile applications. To ensure that devices, systems and applications can trust their respective counterparts it is necessary to identify and authenticate the connected devices in the field as well as the cloud/server side. Authentication can be achieved for example by offering X.509 certificate-based authentication for individual devices by integrating powerful PKI functionality in the IoT platform. PKI is widely recognized as the one of the strongest authentication mechanisms and is therefore a solid foundation for many security elements that protect the IoT solution from the remote device to the business application.

Secure execution environment: Although also true for the server, the ability to manage and execute applications remotely in the field is essential in many IoT applications. For example, over-the-air provisioning and software updates have to be secured. From a technical perspective Open Services Gateway Alliance (OSGi), signed code, and secure boot are just some of the architectural elements that ensure the integrity and security of the overall solution.

Data security: Within the system, data security is the most important aspect to consider. Secure transmission of all data via encryption over an SSL connection is essential. All Console and REST API access must only be exclusively available over an encrypted HTTPS connection. State-of-the-art data centers that utilize the most current architectural and engineering approaches are ideal. All databases should be protected from external access through strict firewall rules. Data should be segregated by account.

Identity and access management: Confidentiality and integrity can be ensured through a role-based access control model and access control lists that follow the Principle of Least Privilege and are enforced through all the layers of the architecture. Each account manages a list of users and controls the user’s credentials. Eurotech’s Everyware Cloud, for example, has a configurable lockout policy per account, which may block a user’s credentials after a certain number of failed login attempts. Logins to Everyware Console can be further protected through the use of a Two Factor Authentication (2FA).

Vulnerability management: Independent certified security firms perform remote vulnerability assessments, including network/host and applications. Vulnerability scanning should be conducted regularly and after any major changes to the infrastructure and environment. Of course addressing any critical security issues found including communicating the problem and solution is important.

Remember, when thinking about IoT security, although data security is essential, do not forget all of those other potential points of failure. From the most remote device in the desert to the backend business system, every part of the IoT solution must be secure.

Eurotech
Columbia, MD
(301) 490-4007
www.eurotech.com
Artila is delighted to announce an innovative IoT automation platform based on ARM Cortex M and FreeRTOS. Unlike Linux that is a full features OS, FreeRTOS is a lightweight real time operation system and a market leading open standard for microcontroller. 

Artila’s Aport and RIO family are based on Cortex M MCU and FreeRTOS and provide a tiny but mighty computing platform which includes real time OS, lightweight IP (lwIP) TCP/IP stack, Web server, serial and I/O device drivers and system configuration APIs.

Aport-212PG serves as a programmable device server which is designed for custom applications such as protocol conversion, remote device monitoring and web based device control. Likewise, RIO-2010PG is also C / C++ programmable and suitable for remote data acquisition and control. Artila’s FreeRTOS Board Support Package (BSP) includes FreeRTOS kernel, lwIP, device driver and configuration library. ARM Keil C / C++ compiler and Sourcery CodeBench lite are supported tool chain and many example programs are available for user’s reference. The Manager utility software is available and used to search and configure Aport and RIO, convert and download the user’s firmware and web page to Aport and RIO.

Thanks to the AJAX and JSON web interface, developing a web based remote I/O control is never so easy before. When a browser sends a request to web server of RIO-2010PG e.g. “GET http://192.168.1.101/wapi/v1/DI/1”, web server will pass this request to AJAX.C to response a JSON data to browser. Then browser can use JavaScript to process the data and update the web page.

Use this FreeRTOS platform, we developed Aport-212 Modbus and DNP3.0 gateway and RIO, web based remote I/O. Artila will continue to develop application ready firmware for users to update the functions of Aport and RIO. iAlarm and iControl are the first two application firmwares available for users to download.

Artila will continuously upgrade our product and service to provide ready to go IoT solution such as MQTT and Cloud applications. Please keep visit www.artila.com for most update news on IoT.

Applications:
- Solar Energy
- Energy Management
- Self Service GAS Station
- Vending Machine
- Data Concentration
- Protocol Conversion
- Front-end Device Control
- Web-based Device Management

**Aport-212PG**

Programmable Device Server
- NXP LPC1768 ARM Cortex M3 100MHz CPU
- 512KB Flash and 64KB SRAM
- 2 x RS-232 / 422 / 485 ports
- 1 x 10/100Mbps Ethernet
- C / C++ Programmable with FreeRTOS
- Support lwIP and BSD socket library
- Toolchain: Sourcery CodeBench Lite

**RIO-2010PG**

Programmable Remote I/O Module
- NXP LPC1768 ARM Cortex M3 100MHz CPU
- 512KB on-chip Flash and 64KB SRAM
- 1 x full modem RS-232 and 1x isolated RS-485 serial ports
- 1 x 10/100Mbps Ethernet
- 1 x serial console port
- Support lwIP and BSD socket library
- Toolchain: Sourcery CodeBench Lite or Keil from ARM
Intelligent IoT Gateway
Reliable Communication Platform for Remote Devices Monitoring

- ARM-based, Linux Ready
- 128MB DDR2 SDRAM, 256MB NAND Flash
- 2 x 10/100Mbps Ethernet Ports
- 2 x High-speed USB Hosts, up to 480Mbps
- 1 x microSD Socket Inside, up to 32GB
- 4 x RS-232 / 422 / 485 Serial Ports
- Extremely Compact Design
- Ultra-low Power Consumption
- Reliable Wired and Wireless Communications
- GNU C / C++ Toolchain for Linux and Windows

Device Cloud

Matrix
Box Computer

RS-232 / 422 / 485

Modbus

Building Automation
Energy Management
Factory Automation
Intelligent Traffic System
Web-based Remote I/O

Artila Electronics Co., Ltd.
Tel : +886-2-8667-2340 | Fax : +886-2-8667-3240 | Email : sales@artila.com | Web : www.artila.com
By 2020, Gartner predicts that there will be 26 billion connected devices. IBM estimates over 100 billion Internet of Things (IoT) devices in the next 20 years. With the rise in connected devices, enterprises are faced with a daunting challenge: how will they extract the value promised by IoT digital solutions without creating even greater security risks for critical infrastructure and machine assets?

The popularity of strategic Industrial Internet of Things (IIoT) initiatives is evident: Digital Oilfield, Smart Grid, and even Digital Factory are just a few examples seeking the transformation of machine data into bottom line value. Universally, these initiatives will depend on the ability to access and extract high fidelity machine data from remote and mobile sources beyond the “four-walls” of traditional data center infrastructure.

Existing industrial M2M solutions all share a common dependence on embedded control system hardware and related systems for access to machine-generated data. These legacy industrial control systems (ICS) are primarily focused on operations associated with critical service levels. Modern, IT-like requirements for dynamic software provisioning, broad IT system accessibility, and robust data exploration capabilities were simply not conceived in the design and implementation of this infrastructure. Yet, these missing requirements are critical to the development of value-driven digital IIoT solutions.

Broadly, industrial OEMs and operators are being challenged with a requirement to embrace a more open network to systems that are tightly integrated with, or even control, critical infrastructure. Traditionally, the ICS infrastructure maintained an “air-gap” policy that effectively restricted connectivity with modern IT/Internet systems. By contrast, IIoT digital initiatives demand data acquisition and access strategies more similar to modern IT systems – bringing wide area networks, the Internet, and Cloud-hosted third party platforms that fundamentally diverge from ICS mandates. For this reason, data acquisition and security challenges are tightly coupled requirements for the development of IIoT digital initiatives. A successful IIoT data acquisition strategy must simultaneously protect legacy ICS infrastructure and enable modern IT security policy and standards.

Exara addresses this challenge by providing edge-based data acquisition services that are isolated from existing ICS infrastructure - providing for high fidelity IIoT machine data acquisition without breaking existing ICS policy. Exara Chronicle software installs to new ruggedized edge servers as a remote data platform tailored to machine data acquisition for high-value industrial assets. Deployed on Intel IDP 2.0/3.0 Gateway devices, the Exara Chronicle software provides the first edge-based data platform design to merge industrial machine data acquisition with modern IT network and access and management. Along with Intel’s embedded security features, Exara adds robust, secure abstraction between machine connections and user data access paths:

- Read-Only by default – no direct access to machines in the data path.
- Process level isolation for all machine protocol drivers.
- Direct API integration for existing IT rights and access management.

Digital IIoT initiatives will demand improved machine data acquisition and accessibility. This signals a shift for IT like data management beyond the four walls of enterprise data centers. This evolution will transform the remote and mobile deployed assets “at-the-edge” into the center of IIoT data management and execution. Exara provides a practical approach to security for core Industrial IoT data acquisition needs by eliminating the conflict between legacy OT infrastructure and modern digital security demands.

Exara
San Juan Capistrano, CA
714.614.7000
www.exara.net
In IoT Security, We Trust

By Gregory Rudy, Green Hills Software

As we come to the end of another summer news cycle, cybersecurity once again saturates the headlines. The summer of 2015 saw cybersecurity vulnerabilities result in the recall of 1.4 million vehicles, the first FDA alert warning, class action lawsuits exceeding half a billion dollars, and more executive resignations. One thing is for certain, customers are demanding better security and starting to hold companies accountable for their designs.

While hacks might not unlock a government supercomputer and wage a real life war, like Matthew Broderick had us believe in “War Games”, what they’ve proved they can do is drive a car off the road, steal personal information, ruin corporate names, and stop hearts. The truth is, the interconnection of our world allows truly amazing movement of information, but those vast and complex connections also provide exponentially more end points, which hackers can use to compromise systems.

This explosion of end points is perfectly represented in the Internet of Things (IoT). At their foundation, IoT devices are all network-enabled embedded systems. They contain inputs, outputs, state machine processing, and data specific to a purpose. Security is typically justified in safety-critical and data-sensitive devices, but what about when it’s neither?

Why care if someone can hack your toaster? The answer is not just burnt toast. A better question is, “What could happen if an attacker changes the software?” Since it’s networked, malicious software can collect and forward network data, such as emails and websites viewed, to someone outside the firewall. If the toaster supports voice commands, software can activate the microphone and record conversations. And that same, once innocuous, toaster can be used to attack other critical systems on the network - your phones, your webcams, and your computers. It’s no longer a matter of your toast -- but your network security.

An end-to-end security architecture protects IoT devices and their networks by establishing trust. Originating from an immutable root allows us to verify that software has not been tampered with or changed. Once we’ve established trust with the software, we can then extend trust to other end points using cryptographic authentication. In this networked world, everything is untrusted until proven otherwise. By limiting software and communication to only trusted sources, we ensure that all IoT devices operate as designed, safeguarding your network from compromise.

The fact is, the Internet of Things is here and growing. This means the number of attack points will continue to increase alongside the number of connected devices. In direct response to this growth, end-to-end security provides the necessary protection to keep the headlines positive. Let’s make sure we drive better headlines in the future.

Green Hills Software
Santa Barbara, CA
(805) 965-6044
www.ghs.com
Basic Security Techniques Really Work

by Alan Grau, Icon Labs

With the building wave of IoT products, services and media coverage, it’s no surprise that IoT security continues to make headlines. Some of the headlines are positive – companies announcing security solutions or standards groups beginning to address security issues; while others are negative – stories of IoT systems being hacked or of IoT device vulnerabilities.

One message that is often lost in the noise is that there are solutions to IoT security, even for the smallest of IoT devices. Security, in many ways, is an arms race; security vendors continue to develop better security solutions while the black hats continue to discover new vulnerabilities. On the other hand, the vast majority of security vulnerabilities in IoT devices are the result of manufacturers failing to include basic security in their products.

Design vulnerabilities are weaknesses that result from a failure to include proper security measures when developing the device, and are the focus here. Examples of design vulnerabilities that have resulted in security breaches include use of hard-coded passwords, control interfaces with no user authentication, and use of communication protocols that send passwords and other sensitive information in the clear. Other, less glaring examples include devices without secure boot or that allow unauthenticated remote firmware updates.

Secure boot utilizes cryptographic code signing techniques to ensure the device only executes code that was produced by the device OEM or other trusted party. Use of secure boot technology prevents hackers from replacing the firmware with malicious versions, thereby blocking a wide range of attacks.

Secure firmware updates ensure that device firmware can be updated, but only with firmware from the device OEM or other trusted party. Like secure boot, secure firmware update ensures the device is always running trusted code and blocks any attacks attempting to exploit the device’s firmware update process.

Utilization of security protocols such as TLS, DTLS, and IPSec adds authentication and data-in-motion protection to IoT devices. By eliminating sending data in the clear, it is much more difficult for hackers to eavesdrop on communications and discover passwords, device configuration or other sensitive information.

Security protocols provide protection for data while it is being transmitted across networks, but do not protect the data while it is stored on the device. Large data breaches have resulted from data recovered from stolen or discarded equipment. Encryption of all sensitive data stored on the device provides protection should the device be discarded, stolen or accessed by an unauthorized party.

Weak or non-existent user authentication has resulted in several high-profile device vulnerabilities including FDA reported medical devices with hard-coded passwords. A strong user authentication method is a clear requirement for device security. Security is a requirement for all IoT devices, no matter how small or seemingly insignificant. By adding a few basic capabilities, the security of any device can be significantly increased. Solutions, including Icon Labs Floodgate Security Framework, exist and are tailored for use in very resource limited IoT devices. These solutions are effective in blocking cyber-attacks. Strong passwords, basic authentication and ensuring the device is running authentic code go a long way to protect IoT devices from cyber-threats.

Icon Labs
Des Moines, IA
(515) 226-3443
www.iconlabs.com
How to Secure IoT Through the Home Gateway

Andy Weitzner, Ikanos Communications

Just like a freight train barreling down the tracks, the Internet of Things can't be stopped. Technologies that show promise to protect us and remove burdens from our lives are inherently desirable. Not only that, but the infrastructure of an industry bent on connecting billions of “things” to the Internet promises to make IoT the largest growth industry in years, or perhaps ever. Still, as with anything new and innovative, but challenging to deploy, there will be bumps along the way.

Along with the complexity of competing IoT standards comes the challenge of security – the security of every one of the billions of connectable devices that are already in use, not to mention the billions more that are on the way.

Quite simply, if those devices provide an entryway to homes or cars, it’s safe to say they are already vulnerable to attack by hackers. A study by Columbia University found security problems in just 2.46 percent of connected business products—but in 41.62 percent of consumer products.

The security problem is multifaceted. Security risks with IoT fall into one of three categories:

- **Taking control of devices** — Taking control of a device can mean logging in as an authorized user, perhaps by figuring out the password, finding a backdoor, or compromising the authentication mechanism.
- **Stealing information** — Stealing information can come in the form of eavesdropping on a system to collect data, such as patient information from a medical device or credit card numbers from a TV used for home shopping. It can also mean commandeering a phone system, printer, or video camera to collect and transmit data.
- **Disrupting services** — Disrupting service usually happens when an attacker floods a system, such as a home-security or vehicle-control system, with messages in order to make it unable to function.

Arguably, device manufacturers who fail to secure their products are experts in product design, but not in security. Or, at best, security is an afterthought. But applying security, like anything else, requires a methodology. Here is a best-practices methodology:

- **Lock down the IoT hub** – The hub can be the central nervous system in an IoT system. It provides direct access to home devices as well as to the cloud. These systems should use a hardened OS and be designed to protect against hacking. A recent study found the need to address these concerns on some popular IoT hubs.

- **Encrypt all traffic** – Strong encryption should be used in communications between devices, as well as between cloud-controlling applications. In addition, stored data should be encrypted.

- **Authenticate and authorize** – Use a firewall to ensure that only authorized traffic is allowed, using a whitelist to limit communication to authorized devices. In addition, it is critical to authenticate users and devices before providing access to any device, application or customer data.

The prpl Foundation recently announced the formal organization of its Security PEG (prpl Engineering Group). The formation of the Security PEG follows months of intensive planning by a subset of prpl members dedicated to defining an open security framework for deploying secured and authenticated virtualized services in the IoT and related emerging markets.

The aforementioned IoT hub can be a weak link in the IoT chain of command. By instead using the home gateway, which relies on a more powerful communication processor, many of these security challenges can be fully addressed.

Some of the challenges that can be met head-on with the home gateway are:

- Support for a fully hardened OS, such as Linux, with powerful firewall and authentication support; hardware encryption that operates at broadband line rates, and secure boot, which eliminates backdoors that hackers can exploit.

Broadband service providers may already have these new or existing powerful systems in place using their existing broadband home gateways. An insecure IoT hub can be replaced by an IoT software package that is installed on a more powerful and secure gateway that has been upgraded with appropriate IoT wireless radios. In addition to security, this ensures a higher level of performance and reliability as well as a longer lifecycle, driving higher end-customer satisfaction.

Ikanos Communication
Fremont, CA
(510) 979-0400
www.ikanos.com
I was recently at a luncheon where the topic of conversation was around the possibilities and promise of the IoT. Can a connected world ensure better health and wellness for the masses? Can we bring about a green future with smart energy across the globe? Closer to home, can we help California through the drought?

The possibilities of the IoT are endless and quite exciting. But each day we see reports of data and system breaches – hacked lightbulbs, vehicles, baby monitors, HVAC systems and more. And with each report, every player in the value chain begins to worry more and more about the integrity and safety of their data and their customers’ data, and as a result about the overall viability of their business in the long term.

Federal and other agencies are already stepping in to regulate this increasingly connected world. The FTC has recommended that Congress enact strong legislation to strengthen existing data security enforcement and notification tools on a federal level. Closer to the hearts of many in the embedded world, it’s been reported that new FCC rules may prevent installing OpenWRT, DD-WRT or other third party firmware on Wi-Fi routers and access-points.

Because of the dozens of governmental agencies vying for a lead role in IoT regulation, large companies are already lobbying to ensure that enacted legislation goes their way. As such, we can see that it’s possible that the IoT could actually become an IoT controlled by a few large companies who have ensured that their platforms and operating systems can play, but potentially leaving the rich ecosystem of open source and embedded tools providers/developers out in the cold.

Legislation and regulation are clearly important in the development of new industries, especially one so fraught with security risks as the IoT, but it’s possible to build IoT products that inherently ensure security while leaving the ecosystem open to all players.

One of the best practices recommended by the FTC is “security by design,” building security into an IoT product early in the design process and at each stage of development. We believe this begins in the embedded system.

Traditional embedded systems are largely closed systems, so security has to date been a fairly straightforward challenge. Static-based approaches have been generally effective, but these approaches are generally CPU-centric, binary (with one secure zone / one non-secure zone), and are complicated to implement. They won’t scale to address the sophisticated types of applications and services being enabled by next-generation connected devices and the Cloud. A more scalable and cost-effective approach is required.

The answer is building multi-domain security into the SoC. Such an approach enables multi-tenant services to work on shared hardware, with isolation provided by hardware assisted virtualization. Virtualization allows for data and execution related to one service to be protected from another. By creating multiple secure domains, each application or operating system can operate independently and reliably in its own separate, trusted environment. This means a compromise affecting one service has no impact to the other.

Such a multi-domain separation-based architecture also eases development and deployment of applications and services. With this approach, developers will be able to securely develop and debug code in a virtualized environment, and operators and other service providers can configure devices for provisioning of services in the field.

Imagine a sensor hub in a home. With multi-domain security, virtualized containers can provide the ability to upgrade each sensor individually – be it home security, door and window actuators, lighting control, appliance management, smart meter aggregation and relay, and more. The system can be designed so that manufacturers and operators can later send software updates to the device, and utility companies can query the device for status – all over the air, and with no possible way for the others to be compromised or to access the other data in the system.

Importantly, such a system can enable separation of networking stacks – Wi-Fi and 6LoWPAN (for example) from the applications running in the other containers. The separation-based approach enables each to be isolated so that certifications remain uncompromised, while keeping power and area to a minimum through integration.

To keep the IoT ecosystem thriving, we need to create and apply portable tools at the foundation level for security. This includes trusted hypervisors, secure messaging channels, security firewalls and more – all built for a multi-domain architecture. The open source prpl Foundation is taking this as its mandate with support from leading companies in the ecosystem, and is progressing this through its Security PEG (prpl Engineering Group). Through an approach called OpenSecurity, the prpl Security PEG is creating open standards and APIs that will help ensure a free and open market for everyone in the IoT value chain, while ensuring security of data and information.

This approach doesn’t address ownership of personal data or other privacy issues (there is still room for legislation!) and we can’t stop hackers from practicing their craft. But with a multi-domain approach to embedded security, we can limit the effects of the hackers by isolating their hacks. And we can let the IoT industry develop organically and robustly through the work of a wide range of innovators and technologies.

Imagination Technologies, Santa Clara, CA (408) 530-5000. www.imgtec.com
prpl is Pragmatic for Security

by Simon Davidmann, Imperas Software

Most of the public discussion about security presents various aspects of the problems, or a high level view of risks/solutions, or an individual company’s solution to their slice of the problem. The prpl Foundation’s Security Working Group is taking a pragmatic, cross-functional approach to security in embedded devices and systems.

What do I mean by pragmatic and cross-functional? Let’s start by looking at the two primary approaches to security in systems. The first is a layer by layer approach, where the working assumption is that if each layer of the system is secure, then the system will be secure. The second approach is to take a “world view” of security, and try to solve the complete system security problem. With the first approach, it is unclear that the layer security assumption is correct, and even if it were correct, this would be expensive (in dollars, power, performance) to deploy on billions of IoT devices. With the second approach, it is impossible to start from a world view and arrive in a reasonable time at a set of security practices that can be implemented.

With this in mind, the Security Working Group has brought together companies and individuals with expertise in various aspects of embedded systems and security to document current best practices and derive a set of recommended new security practices for embedded systems. This cross-functional group includes representatives from processor IP vendors, embedded hypervisor/OS developers, secure application developers, semiconductor vendors, software/systems tool vendors, systems companies and security experts. Each brings their own experience and expertise to the group, hopefully enabling whole-is-greater-than-the-sum-of-the-parts results.

Imperas is a developer of software debug, analysis and verification tools based on virtual platform technology. Virtual platforms in general bring a number of advantages to work in this area, including the ability to develop software and systems before the hardware is available, and controllability, observability and repeatability of simulations including both hardware and software.

Imperas specifically brings to this party the largest library of processor core models from our Open Virtual Platforms (OVP) initiative, and a simulation infrastructure that enables non-intrusive tools to be built with low overhead. Also, we bring to the group our experience working with nearly 20 different hypervisor, OS and secure application developers, and our understanding of the tools and analytical capabilities they need. Our contribution will be to enable the prototyping and testing of new hardware, software and system approaches to embedded security, and to provide demo platforms to both group members and the larger embedded community.

Here are three examples of areas where Imperas expects to contribute to, and collaborate with, the group:

1) Porting of security practices to a variety of processor cores and devices. While Imagination Technologies is a member of the Security Working Group, and initial work will focus on their MIPS cores, the Imperas OVP Fast Processor Model library includes over 150 models of different processor cores. Virtual platforms will be used to port and bring up a secure software stack on new virtual hardware, and demonstrate that the recommendations resulting from the group’s efforts apply broadly to embedded systems.

2) Development of tools to test the software stack and the security of systems. These tools could provide insight and optimization for hypervisors or secure applications taking advantage of the new hardware virtualization instruction extensions in MIPS and other cores. Or the development of assertions in the virtual platform simulation environment to test that guest operating systems and applications running on hypervisors stay strictly in their assigned “containers.” Or the development of specific fault injection tools to test system recovery from a security breach. Or …

3) Development of Extendable Platform Kits (EPKs) as demonstration and test vehicles for security best practices. EPKs are virtual platforms, including processor models plus peripheral models necessary to boot an operating system or run bare metal applications. The platform and peripheral models included in the EPKs are open source, so that users can easily add new models to the platform as well as modify the existing peripheral models. The example software stack also included. A block diagram of a MIPS-Linux EPK is shown in Figure 1.

At Imperas, we’re excited about the practical approach to security being taken by the prpl Foundation’s Security Working Group, and look forward to contributing our own unique skills and technology to the team.

Imperas Software
(925) 519-1234. www.imperas.com
Solving IoT Security Problems with New Generation of FPGAs

by Tim Morin, director of marketing, Microsemi

It can be extremely challenging to combat design cloning, reverse engineering or tampering in today’s IoT. FPGAs help by including security-focused features that add defense at the device level. These include a physically unclonable function (PUF) from which the Private Key in the Public/Private Key scheme can be derived for implementing M2M authentication using Public Key Infrastructure (PKI). Other important features include cryptographic accelerators, a random number generator, and Differential Power Analysis (DPA) countermeasures that, together, allow system architects to layer security throughout the system.

The multiple electronic networks of the IoT require end-to-end layered security, starting at the device level. FPGAs help deliver this layered security by including unique built-in features and differentiated capabilities, and by becoming the root of trust in very complex applications.

A major benefit of flash FPGAs is that a flash FPGA stores configuration information on-chip in non-volatile memory, preventing anyone from capturing information for reverse engineering or design tampering during device configuration. The FPGA must protect all data including the application data that it is processing. This requires numerous data protection features including hardware protection from differential power analysis (DPA) and other side-channel attacks. Simple and differential power analysis (SPA/DPA) can be used to extract secret keys by measuring power consumption during cryptographic operations like bitstream loading. Not only is it important to provide countermeasures to side channel attacks, it’s also important that systems are assessed as to their claims. Microsemi SmartFusion2 and IGLOO22 FPGAs are the only FPGAs to achieve CRI DPA logo certification.

Also important is machine authentication using a PUF to generate a private public key pair. Analogous to a human fingerprint, the PUF serves as an unclonable “biometric” identifier unique to each device.

An SRAM PUF (Fig. 1) measures the random start-up state of the bits in an SRAM block. Each SRAM bit comprises two cross-coupled inverters that are nominally equal but not completely identical. As power is applied to the IC, each SRAM bit starts up in either the “one” or “zero” state based on a preference that is largely determined during IC manufacturing.

The SRAM PUF can be designed to guarantee perfect key reconstruction with exceptionally low errors, and the SRAM PUF’s secret key is extremely well protected since its secret effectively disappears from the device when the power is off. No amount of subsequent analysis will reconstruct the PUF secret key if the activation code is erased.

FPGA or SoC FPGAs with PUF technology must also include built-in cryptographic capabilities -- i.e., hardware accelerators for AES, SHA, HMAC and elliptic curve cryptography (ECC) -- as well as a cryptographic-grade true random bit generator. This ensures that a user PKI can be created with the user’s own certificate authority blessing each legitimate machine in the network. Each machine has a chain-of-trust extending from the user’s well-protected root-CA keys to the PUF’s high-assurance, atomic-level identity. Every machine and their communications are protected and can be safely, securely and confidently used in M2M, IoT and other hyperconnected applications.

Microsemi
Aliso Viejo, CA
(949) 380-6100
www.microsemi.com
Need a new reflective memory solution

PCI Express® Network

Dolphin's PCI Express® Network is the right choice for high speed reflective memory solutions. Distribute data with the lowest latency and highest throughput.

PCI Express Multicast
Dolphin combines PCI Express multicast with our SISCI API. The combination allows customers to easily implement applications that directly access and utilize PCI Express' reflective memory functionality. Applications can take advantage of latencies as low as 0.99 µs and throughput at 2650 MB/s. Combined with PCI Express peer to peer functionality, FPGAs and GPUs can distribute data to multiple nodes without the use of a CPU.

Learn how PCI Express™ improves your application's performance

www.dolphinics.com
Embracing ARM in the Cloud Datacenter

What ARM’s arrival in the datacenter means for scale-out Cloud platforms and the processor marketplace that services them

by Karl Freund and Dilip Ramachandran, AMD

Cloud datacenter infrastructure is proliferating quickly, driven by exponential data growth and the hyperscale elasticity needed to accommodate rapid fluctuations in Cloud compute workloads and long-term capacity plans.

These scale-out, dense-server Cloud platforms are tiered across application-optimized software stacks, underpinned by flexible pools of homogeneous server, networking and storage infrastructure designed and configured to meet exacting performance-per-watt targets. For Cloud operators, bottom line revenue is sharply aligned to aggregate I/O, power consumption and associated costs. Space savings, compute density and thermal versatility play important roles in the equation.

In parallel, reflecting the growing popularity of open computing platforms, datacenter architects increasingly seek greater ‘openness’ at the server processing layer. They naturally want the freedom and flexibility to source processors from multiple vendors, giving them greater leverage to negotiate performance specifications, power profiles and pricing. They also seek a healthy, established software ecosystem that can rival the x86 software ecosystem for robustness and longevity.

They needn’t look far.

Enter ARM

The arrival of server-caliber 64-bit ARM technology marks a pivotal change in the Cloud infrastructure market, and will help fuel massive multi-vendor innovation around ARM processors’ core building blocks. With products leveraging ARM processors coming to market from AMD and others in variants from ‘brawny’ to ‘wimpy’, Cloud datacenter designers stand to benefit from an expanded array of processing performance options to meet highly targeted workload needs at competitive price points and with significant power efficiency. Allocated to the appropriate applications, ARM can provide long term strategic value.

Cold data storage is a good early candidate for ARM processors. Put simply, you don’t need high performance x86 processors to occasionally transfer small volumes of data from hard drives to the network. You need enough processing power to
support CRC calculations and other data integrity measures, but x86 processing may be overkill. Server-caliber ARM processors can provide more than enough processing performance for these functions, with additional options for further maximizing I/O. AMD’s ARM-based solution, for example, integrates 14 SATA ports with integrated connectivity to disk drives.

Media streaming is another compelling use case for ARM. Here you need “good-enough” processing performance to ensure smooth multimedia content delivery, while balancing compute density and costs against hyperscale content and throughput volumes. Single chip ARM-based SOCs at the server processing layer will provide significant power efficiency and thermal benefits that enable low power, high density racks to stream at the requisite I/O with a low cost of ownership.

Web applications written in PHP or other high level programming language are good candidates for ARM. These apps aren’t machine dependent and can therefore run on ARM or x86, so any kind of LAMP stack application just runs, no code recompilation required. If you’re currently using FORTRAN or C++, it will be necessary to recompile, and this is where the software community will take time to validate and support ARM. But for an enterprise with a lot of end code written in Java, for instance, it will be able to get software up and running quickly on ARM.

Using ARM, big web properties with hyperscale compute resources – such as Google, Baidu, Facebook, Amazon Web Services, etc. – could translate even relatively small performance per watt gains into huge aggregate financial benefits. These entities are particularly well attuned to the value of open architectures, and are keenly interested in exploiting this trend at the processing layer.

For datacenter operators running high-concurrency workloads on dense front-end web servers, ARM-based processors can also counter some of the performance degradation issues that arise from the inefficient use of x86 processor caches, while simultaneously offering power efficiency and high server processor density. A significant number of datacenter workloads have inherently low instructions per clock (IPC) and high cache miss rates. For these workloads, ARM-based processors with smaller cores and caches can enable the equivalent performance as traditional server processors with large cores and caches, while minimizing power and area requirements.

The research and academia domain will take a leadership role in evaluating and implementing ARM for high-performance computing (HPC) applications, which, to date, have been dominated by high-performance x86 processors. Commodity ARM processors have already made inroads into this domain, as evidenced by the Barcelona Supercomputing Center’s (BSC) selection of low power ARM-based Samsung processors to build a new supercomputer. Via its Mont-Blanc initiative, BSC is endeavoring to build a 200 petaflop system that uses only 10 MW of power. Though ARM isn’t a likely candidate in the short term for matrix multiplication-intensive applications like neural networks or machine learning, it can be well suited for the numerous single-purpose HPC apps that don’t need floating point precision but do need improved power efficiency.

Network function virtualization (NFV) is another attractive use case for ARM-based processors, enabling networking/telecom service providers to simplify infrastructure deployment and management via a fully virtualized communications framework (Figure 1). With NFV, much of the intelligence currently built into proprietary, specialized hardware is accomplished instead with software running on general-purpose servers. By abstracting network devices such as routers and gateways within a virtual server, storage, and network environment, core network functionality can
be scaled and managed with newfound agility. And by minimizing dependencies on customized, integrated hardware, operating system, middleware and application stacks, service providers can also accelerate development cycles and help avoid vendor lock-in.

ARM-based processors are particularly well suited for NFV in part because they can be tightly mated to network interface controllers in silicon. This results in NFV-optimized SOCs that consume minimal power while providing significant space-saving benefits. This latter attribute is particularly valuable for field-deployed telco equipment in dense metropolitan environments, where a pole-mountable, shoebox-sized system is far more desirable to deploy than a floor-standing, cabinet-sized system.

Working with companies like ENEA, AMD is helping pave the way for service providers to design and deploy NFV infrastructures such as Open Platform for NFV (OPNFV) on ARM. Leveraging advanced software-defined networking (SDN) capabilities, NFV holds the promise to meet exacting network performance, management flexibility, and cost requirements. Initiatives such as OpenDataPlane (ODP) open source project help the cause by providing open application programming environments that are portable across networking SOCs of various instruction sets and architectures.

ARM is also distinguished by its robust security capabilities, which stem from its extensive use in mobile device applications. The ARMv8 architecture takes these capabilities a step further, particularly with regard to encryption and decryption processing efficiency, while simultaneously introducing 64-bit ARM support for datacenter infrastructure already accustomed to 64-bit x86 computing. ARMv8 cryptography extensions incorporate instructions to accelerate Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) cryptography algorithms. This native, hardware-based cryptography support avoids the performance, power and cost penalties introduced via pure software-based implementations, and can complement existing hardware accelerators.

ARM-based processors that are enabled with TrustZone technology can allow the establishment of key-protected zones of multiple computing devices that operate as unified security zones, backed by hardware based access controls. This ability to support multiple independent security profiles with a single core is a compelling feature for datacenter architects seeking to build a secure private network, implement advanced DRM schemes, or establish a trusted boot capability, for example.

Evolving with ARM

Momentum continues to grow for ARM in the Cloud datacenter, yielding significant industry advancements. Red Hat recently made its Red Hat Enterprise Linux (RHEL) Server for ARM Development Preview available to members of its ARM Partner Early Access
Program, providing a common standards-based operating system for existing 64-bit ARM hardware. HP recently announced its first ARM-based servers, and AMD’s first 64-bit ARM implementations – high-performance, low power K12 cores, AMD Opteron A-Series ‘Seattle’ server processors, and AMD Embedded R-Series ‘Hierofalcon’ SoCs – are on the near horizon.

ARM penetration and propagation into the Cloud datacenter will be facilitated in part by its vast, established software ecosystem. Continued innovation in open source software enablement and complementary virtualization technologies will further advance the transition to Cloud datacenter infrastructure based on both x86 and ARM processor platforms, aligned appropriately to the applications that stand to gain the most performance and/or power benefits from each architecture.

Leveraging ARM at the processing layer, dense-server Cloud datacenters can scale out more flexibly and power efficiently, reducing total cost of ownership. Equally important, with ARM, datacenter architects now have the freedom to choose processors from a wider, more open, and more competitive marketplace.

ARM
Cambridge, UK
+44 (1223) 400 400
www.arm.com

The Right Security for IoT

Protect Your Embedded Project with the OPTIGA™ Product Family

Security is more than data protection – in many cases, security measures also enable new business models and services such as remote feature management. However, performance and security requirements vary considerably from one embedded project to another.

To reflect this diversity, our proven OPTIGA™ family allows you to match security functionality to your specific application needs. Designed for ease of integration, this proven, scalable family ranges from authentication solutions to more advanced implementations.

For more information call 1.800.981.8699 or visit www.infineon.com
Securing Consumable Components in an Embedded System Design

Consumable components come with unique security challenges. Designed to be installed new and consumed through one or more cycles of product use before ultimately disposed and replaced, consumable components are incorporated into a variety of embedded systems—from medical devices to printers.

Consumable Authentication

A secure communication protocol includes the following three areas: First, the base unit must be able to distinguish an authorized consumable from a clone. Second, the mechanism should have the ability to limit usage time and/or count uses of the consumable. Finally, the base unit should be allowed to reject spent consumables. In order to provide a concrete example, consider the design of a medical device as shown in Figure 1, which consists of a terminal with which a doctor interacts through a user interface and a limited-use surgical implement that interfaces directly with the patient.

When using the medical device as an example, it’s easy to see how vital it is for the terminal to be able to authenticate the consumable. Perhaps each consumable contains secret information known only to engineers working for the manufacturer of the system. Furthermore, each consumable might contain a serial number or encryption key that is unique. Of course, this means that these secrets must be carefully protected, whether they are sent over a communication channel or not. A determined (and well-funded) attacker, after all, can generally observe real-time communication over cables between the terminal and consumable, examine the contents of read-only memory areas, and disassemble executable code.

After the medical procedure is completed, the attached consumable must somehow be “marked” as used—either via the consumable itself during the procedure or through a command from the terminal afterwards. The first approach is generally more secure, but it’s not foolproof either. For example, say that a medical consumable is set to a limit of “single use,” defined as one successful session on a single patient. But what if that procedure involves several runs using the same consumable?

Finally, when the consumable has been used to its capacity and therefore should be disposed, the terminal should be able to reject an authentic product.

Even when the three elements above are in place, though, a designer must consider the possibility of certain well-known protocol attacks. For example, in a classic "replay attack", the designer of a clone device could simply record the responses of an authentic and unspent consumable to the various commands from the terminal and replay those same messages from the clone. Alternatively, a third party might attach a spent consumable to the base unit by way of a special "black box" device that would intercept and sometimes alter otherwise genuine communication between the two endpoints as illustrated in Figure 2. This approach is commonly referred to as a “man-in-the-middle” attack.
In order to prevent such attacks, an off-the-shelf authentication chip can be placed on the consumable to provide a tamper-proof private key management solution. These types of devices typically offer multiple security models, such as a random challenge/response, that are based on open cryptographic standards and can eliminate the need for a processor on the consumable. Some manufacturers offer implementations that use a single line for communication and power along with a ground reference, which can be a real advantage when the number of pins is at a premium on the consumable connection. Application specific data storage is also available and can be configured for “one-time programming” mode to track usage. This specific feature can be employed to prevent attackers from resetting the usage count on a spent consumable. Other methods of authentication could include monitoring the power consumption profile of the consumable and looking for uniquely identifiable behaviors.

The Art of Reverse Engineering

In order to protect yourself against an attack, it’s important to know the techniques attackers use in the first place. One of these techniques is known as a “chip rip,” whereby they physically remove the top of a chip and analyze its internal structure for data, such as a private security key. There are a variety of ways to prevent this type of attack: Some chip vendors offer “tamper proof” solutions for their products while contract manufacturers can use other mechanical defenses against this type of attack. Finally, a process called “chip sanding” can also be employed to eliminate any identifiable markings, thereby complicating the identification of the device.

Another effective method used by attackers is to connect a debugger to the system processor and step through code execution in order to determine a variety of vulnerabilities. This threat can be reduced by disabling the JTAG port,—through burning fuses or writing specific values to locations during device programming—or configuring the appropriate debug registers early in the boot process. It is also important to remove all debug connectors/pads along with any related test points. Detection is key to countering this type of attack, through the use of case interlocks, destructive enclosures, clock speed and/or voltage level monitoring, and validating the code image by the use of a digital signature. When an intrusion is detected, the system could potentially log and/or report the attack and optionally cease to operate.

Given the level of attacker sophistication, designers must avoid using simple methods like recording serial numbers of each consumable in a text file on internal or removable storage. This type of approach to security is easily exploited by less-sophisticated attackers. Other methods that involve security by obscurity are also generally easy to circumvent by experienced attackers. However, by carefully applying multiple levels of effective security measures, designers can slow down attackers and protect against a single point of entry if a specific tactic is weakened or broken.

Upgrading Security in the Field

As consumables become more and more profitable, there will be increased risk of reverse engineering. If there is sufficient economic incentive, a determined attacker will find the weakest link. To limit the manufacturer’s risk, it is critical to quickly retrofit additional security. If the exploit can be prevented by modifying only the consumables going forward, that is ideal. If the exploit can only be prevented by upgrading the terminal, then this must be planned for in advance. Ideally this could be accomplished through a software update, but that is not foolproof as the updates may not be applied by the end-user in a timely fashion.

Securing a software update requires three aspects: authentication, validation, and secure boot. Authenticating the new firmware before it is installed and validating it after it has been programmed into flash is key. So is having a secure boot strategy. This is a feature of the processor along with immutable and often multistage authenticated boot images that prevent unauthorized code from executing. Regardless of the software update delivery mechanisms (Internet, USB, SD Card, serial) and whether the end user or field technician performs the upgrade; these three aspects are critically important to preventing an attack.

Finally, the use of code image hashes, public key signatures, and signature authority certificates are common and proven methods to ensure authenticity. There are many providers of tools, processes, and hardware that take full advantage of this standards-based approach. In addition, researchers are constantly developing new and innovative ways to increase the level of security in a variety of settings while leveraging existing standards where possible. An example of this would be the creation of SHA-2, which is a cryptographic hash function defined by the NSA and published by NIST as a US Federal Information Processing standard. It increases the number of output bits in SHA-1 from 160 to 256 bits and beyond in a variant based on...
roughly the same underlying mathematical concepts.

**Pragmatic Example**

As described in the previous section, one method of authenticating a consumable is to use an off-the-shelf 1-Wire authentication chip. 1-Wire is a device communication bus system originally designed by Dallas Semiconductor Corp. that provides low-speed data, signaling, and power over a single signal. This approach keeps the complexity and cost down on the consumable side and shifts the burden to the terminal side in terms of implementing a random challenge/response protocol. A high-level illustration shows the primary functional blocks in Figure 3.

In this example, a private key is permanently stored in the authentication chip during manufacturing and is unreadable from the 1-Wire interface or through physical tampering. A random challenge is generated by the processor on the terminal side and is submitted to the authentication chip over the 1-Wire interface. The consumable provides a response back to the terminal based on the private key. The response is then compared to an expected value that was computed by the terminal's processor, using its protected copy of the same private key, which is a concept commonly referred to as “symmetric keys”. If the response matches the expected value, then the consumable is authenticated as genuine and normal system operation can continue. The terminal may also repeat this authentication process randomly to make sure that the device has not been swapped out with an unauthorized consumable during the course of a given treatment session.

If the selected processor does not provide any inherent security features, then a second authentication chip can be co-located on the terminal to provide the required functionality. Aside from a secure key storage solution, all of the needed features can alternatively be leveraged from off-the-shelf software libraries. However, keep in mind that this will have an impact on processor performance and memory footprint.

Once the device has been authenticated and before a treatment session begins, the processor checks that the current usage count on the authentication chip data store is below a defined threshold. If the threshold is exceeded, the terminal will not begin the treatment session and consequently inform the operator that a spent consumable has been attached. Otherwise, the terminal will increase the usage count on the consumable by using the “one-time programmable” feature (bits can only be set to ‘0’ once, so successive bits are used to implement a count) of the authentication chip and the treatment session will begin. On some systems, the threshold may be determined by using a time stamp with a duration limit as opposed to or in addition to a session counter.

In this example, it also may be important to encrypt patient and general communication data to/from the consumable. This can be accomplished with either the same private key, or a different key stored on the authentication chip. Depending on the type of data and rate of communication with the terminal, the consumable would likely require a dedicated local processor and/or custom hardware to implement the encryption and decryption algorithms. Conversely, the terminal would need to have sufficient resources to process the encrypted data in real time.

As consumables are becoming more and more profitable, they will continue to be attractive targets for would-be attackers—at the same time, the attacks themselves are becoming more sophisticated. All hope is not lost, though: Due diligence on the part of designers can go a long way toward preventing these attacks.

To prevent unauthorized cloning, a consumable must be authenticated as genuine through a secure communication protocol. In addition, the consumable must have a method for checking and updating its usage count and/or time stamps so that it cannot be placed in service beyond its intended life, which for most medical devices is a single “valid” use.

Employing counter-measures like removing debug connectors, tamper detection, and using tamper-proof components and/or other mechanical defenses can dramatically increase the level of difficulty for physical attacks.

Finally, to prevent unauthorized code from executing on the system, it’s important to consider retrofitting additional security. Authenticating new firmware before it is installed, validating it after it has been programmed into flash, and having a secure boot strategy are key.

Protecting a consumable against an attack may take extra effort and cost upfront, but it’s worth it when you consider the cost of a security breach. Consider all of the applicable risks such as safety, litigation, quality, terminal damage, support, reputation, and lost revenue. Can you afford to take this level of risk with your consumable?

**Barr Group**

**Germantown, MD**

(866) 653-6233

[www.barrgroup.com](http://www.barrgroup.com)
High Performance Computing Appliances

Attach incredible compute power and flash storage to your servers.

Compute Accelerators
- 3U rack space
- Four removable canisters containing 16 K80 GPU cards
- IPMI system monitoring
- 6,000 watts of n+1 redundant power
- Superior cooling with temperature controlled fans
- Direct attach with four PCIe x16 Gen 3 cable connections to host server(s)

CA 16000
adds over 79,800 cores and 139.8 TFlops
with NVIDIA® Tesla® K80 GPU accelerators

OSS Compute Accelerators are qualified to operate with OSS EOS server, Intel S2500CO, Supermicro 7047GR-TTR, Dell R720, and IBM 3650-M4 servers operating NVIDIA Tesla™ GPU’s. They can also be pre-configured with Intel Xeon Phi™ Coprocessors.

Flash Storage Arrays
- 3U rack space
- Four removable canisters containing 32 Flash cards
- IPMI system monitoring
- 2,400 watts of n+1 redundant power
- Superior cooling with temperature controlled fans
- Direct attach with four PCIe x16 Gen3 cable connections to host server(s)

FSA 200
provides 200TB All-Flash storage delivering 16 million IOPS

877-438-2724
sales@onestopsystems.com

One Stop Systems sales engineers are available to help you configure the exact system to meet your specific requirements.

See all our products for HPC at
www.onestopsystems.com
It is very impressive how computing power increases year over year. Previously this was achieved by running at higher and higher clock frequencies, and then by going to smaller structures and now by constantly increasing the numbers of CPU cores in a package.

When looking back, and really only about 10 years, x86 single-core processors burning somewhere between 30 and 60 watts were top of the line in embedded system design. Now quad-core processors are doing their job in industrial PCs requiring less than 10 watts. While processors have been growing rapidly in performance, computer memory has a hard time keeping up. It is important to understand that in addition to computing power, memory access time and throughput plays an essential role in total performance. As CPUs can process data much quicker than they can access main memory, memory access very often turns out to be the bottleneck in a system. When processing only a small amount of data, and when multiple levels of cache are available, this performance-limiting effect is greatly reduced and therefore hardly noticeable. But when processing large amounts of data, problems arise.

In contrast to multiple Gigabytes of main memory, caches can only hold some kilobytes (or maybe up to a few Megabytes) of data. When data not found in cache needs to be accessed, so called ‘cache misses’ can happen, meaning the processor has to access main memory to load data and at the same time push already-cached data out of its caches. Pushing data out of the cache also usually includes data required for time-critical processes. Because this data has to be reloaded again later, determinism is greatly affected—which in many embedded systems is deadly. In a real-time operating system, this phenomenon also leads to an increase in latencies. Processing interrupt requests may be delayed if code associated with an interrupt has to be reloaded from memory, and in addition to high interrupt latencies, prolonged task-execution times in general can be observed.

In a perfect world, time-critical real-time code would always be kept separate from non-deterministic code. A good example would be the deployment of a non-real-time operating system like Microsoft Windows in parallel with a real-time operating system (RTOS). In this case a hypervisor can address jitter related to competing cache and memory access by giving an RTOS priority over Windows. The RTS Hypervisor from Real-Time Systems for example supports this functionality, and has done so since early 2014 and other hypervisors are sure to follow on the market.

On high-end systems, where multiple real-time operating systems are run and multiple processor sockets are available on a board, latencies due to memory access can be even further optimized or eliminated by using a hypervisor optimized for Non-Uniform Memory Access (NUMA).

In a NUMA system, every processor holding from four to 36 logical x86 CPUs has its own memory controller on-chip for accessing main memory. All processors on each board are then linked to each other via fast point-to-point interconnects. Individual processors, including their local memory bank(s), are called NUMA-Nodes. Figure 1 illustrates an example of a NUMA system similar to the one used in the measurements below.

In a NUMA system, memory access time depends on the memory modules involved, or more precisely, on which processor the physical memory bank in question is connected to. Each processor can access any memory module on a board via the processor-to-processor interconnects. Accessing local memory banks via the processor’s own memory controller is of course faster. Thinking this through, the advantage seems obvious: If every CPU processes its data using its own local memory, no processor would impact any other processor, neither through cache misses nor through competing access via the same memory controller.

In order to optimize memory usage, some operating systems feature “NUMA Support”, allowing applications to be distributed to various NUMA nodes exclusively. And, for some applica-
In NUMA systems, every processor has its own memory controller on chip.

In NUMA systems, every processor has its own memory controller on chip. This approach does work well, but as always, the devil is in the details: When analyzing operating system functionality (like scheduling, page fault handler, device drivers including interrupt processing), chances are that some operating system code is being executed on a different node than the one requiring this functionality at that time. When running number-crunching applications, this usually does not cause much of an impact, but in real-time applications it is exactly these system calls that make up an essential part of the code. If execution of applications are really to remain independent, clean partitioning of resources is absolutely required. Consequently, this can only be achieved by running multiple operating systems in parallel.

Starting a separate operating system on each of the physical processors can be accomplished using a Type-1 hypervisor—a hypervisor that runs without host operating system directly on the hardware, also called “bare-metal hypervisor.” Still this does not quite satisfy the above requirements. In order to provide determinism and maximum performance, the hypervisor in use has to be NUMA-aware, meaning that memory allotment has to be done the right way by physical address of memory required by the hypervisor itself and for each guest operating system. This is the only way to really avoid the problems described above caused by parallel execution and concurrent memory access.

Because NUMA-aware hypervisors for real-time use were not available in the past, the RTS Hypervisor was advanced by adding specific NUMA functionality and configuration capabilities.

The previous RTS hypervisor offered two different modes for running guest operating systems (Guest OS): A "fully virtualized" mode, typically used for running unmodified general purpose operating systems (GPOS) and the so-called "privileged mode" for executing operating systems deterministically with direct hardware access in hard real-time.

While both modes allowed direct assignment of available processor cores, logical CPUs and devices to operating systems, memory partitioning optimized for NUMA was not possible. Both modes did not provide the desired behavior: In virtualized mode, the hypervisor added a software layer between Guest OS and hardware, potentially adding latencies, affecting determinism and introducing some jitter. In “privileged mode” on the other hand, hard real-time and direct hardware access was guaranteed, but without virtualization, physical memory location could not be chosen for a Guest OS at will.

Typically, an operating system is linked to a specific base address and usually needs 32-bit addressable memory somewhere below 4 GB. To support the NUMA architecture a third mode of the RTS Hypervisor was required, a “privileged mode” with virtual memory management unit (MMU). This mode adds minimal virtualization, only for virtualizing the guest operating system’s memory access. In virtual MMU mode a guest OS can then be moved freely to any location in physical memory even allowing, for example, a 32-bit operating system to run at a location that usually is far beyond its addressable range. By means of the virtual MMU mode it is therefore possible to execute multiple operating systems, requiring the same physical addresses for their kernels simultaneously in parallel while using all of the available physical memory of the system.

The underlying technology is called “second level address translation" which is available in current processors supporting virtualization from both Intel and AMD. Intel named it Extended Page Tables (EPT) and AMD calls it Rapid Virtualization Indexing (RVI) or nested paging. In virtual MMU mode the hypervisor warrants that execution of a guest OS is not interrupted by hypervisor code, i.e., without additional latencies. Only if a guest OS were to access memory outside its pre-configured allowed address ranges, would the hypervisor step in. To avoid any influence on other NUMA nodes, all required page tables and structures of a guest OS are automatically loaded in memory of the same NUMA node by the hypervisor.

The Results

When designing real-time critical systems, assumptions and theoretical considerations never replace real-world measurements and long term tests, which is why the following tests on a real system were performed:

The test platform used carries four Intel XEON E7 ten-core processors with hyper-threading, linked to each other via QuickPath Interconnect (QPI) as pictured above. Each QPI link offers a maximum transfer rate of 6.4 Giga transactions per second, which translates into 16 GBytes per second considering the 20-bit width of the QPI. As always in hyper-threading pro-
cessors, two logical CPUs of a given processor core share their Level 1 caches (32KBytes). Each processor core then features its own Level 2 Cache (256KBytes) and all 10 cores of a processor use the same Level 3 Cache (24MBytes). Each processor with its associated memory represents one NUMA node holding two registered DDR3 1066MHz SDRAM modules each. Two NUMA nodes have a direct link to the chipset (Node 1 and 2).

As guest operating systems, a real-time Linux with kernel 3.12.42-rt58.x86_64 was run in multiple instances in parallel. In the hypervisor configuration for each guest OS instance a different NUMA node was selected for it to run on. Whether memory directly attached to the assigned node is used or if memory of other NUMA nodes should be used can be selected as well.

When measuring throughput, the difference between accessing local memory attached directly to an operating system’s own processor vs. accessing memory on a different node via the QPI can be seen clearly in Figure 2. The measurement shows bandwidth results using 128-bit read cycles (Load MMX register from main memory using a variety of block sizes). When reading blocks larger than the size of the cache, the difference in bandwidth depending on memory location can be observed clearly. The steps in the resulting diagram represent the different levels of cache, 32KB and 256KB Level 1 and Level 2 cache. Beyond 24MB block size (extend of Level 3 cache) the actual bandwidth of the path to main memory can be seen, roughly 4.7 GByte/s vs. a little over 3.6 GByte/s.

While bandwidth is of course of interest, even more important in embedded and real-time applications are latencies, determinism and jitter. In order to measure latencies caused by simultaneous access to memory by multiple operating systems a special software program was used. This test program allocates a 64 MB block of memory, substantially larger than the 24 MB last level cache to minimize cache effect. The test tool then writes the first DWORD (4 Byte) in steps of 4096 Byte (one page). After this, in a second loop all previously written data is read back.

This measurement is executed in kernel mode with all interrupts masked. The measurement illustrated in Figure 3 shows two operating systems, running on separate cores but on the same NUMA node. Basically this scenario could be viewed as a traditional non-NUMA System without using memory access prioritization described in the beginning of this article. Operating system 1 executes the test program described above while the second OS is idle, illustrated in green color. The duration of the memory loop stays at a constant value of about 1140 µs. If the second operating system now executes memory benchmark software, the red curve shows the resulting memory loop duration. The load created on the memory bus by the second operating system has a massive impact. The loop duration takes up to 5800 µs, a factor of 5 of the original time it took.

In our next examination of the system, we started the second operating system on a different NUMA node. In our measurement (Figure 4) it shows that even if a heavy load is applied to either operating system, there is a clear separation and no influence between the individual nodes. The curve of the observed memory loop durations closely matches the results of the “no load” scenario above shown in green.

The measurements that were performed attest that memory access can be optimized using a NUMA-aware bare-metal hypervisor combined with intelligent physical memory management. Access time to RAM can be reduced greatly if only memory modules connected to a processor’s own on-board memory controller, i.e. on the same local NUMA node are used.
Figure 4
Assigning memory exclusively, max. execution time is not affected under load

Very drastic improvement can be achieved for memory intense applications. If a lot of memory transactions and parallel access to memory are required, separating traffic (i.e., keeping each NUMA-node autonomous) has a huge impact on the execution time. Without NUMA-awareness in the hypervisor, the maximum execution time of the test program went up by a factor of 5.

As a conclusion it can be said: “Making the Most of Multicore” involves smart handling of memory. If virtualization is used on small, embedded systems, for example, one featuring only one dual-core Atom processor and a single memory module, then prioritization of cache and memory access is a must in hypervisor functionality. On larger systems, the hardware design is already laid out to separate caches and memory controllers, but only hypervisors or virtualization that is NUMA-aware can make effective use of this architecture.

Real-Time Systems
Ravensburg, Germany
+49 (0) 751 359 558 – 0
www.real-time-systems.com
With the rise in availability of multicore embedded processors, especially those offering virtualization support, it is likely that the embedded world will follow the enterprise world and embrace the use of virtualization.

It’s becoming more and more difficult to buy a single core 32- or 64-bit processor, and given that most embedded systems have traditionally run on single core processors, what happens when it's time for a hardware refresh? This really comes down to a software decision and typically a decision on what sort of platform software should be used to make the best of the new multicore hardware.

The first option to consider is using a real-time operating system that supports multicore processors. This RTOS would seamlessly run the application code over the different processors using a symmetric multi-processing (SMP) scheme. The scheduling and management of the multiple cores is left to the RTOS and the developer often has very little to do to enable the extra processing power now given to him. The issue really becomes the ease of portability of legacy software applications, and how easy it will be to bring these applications over to a new SMP RTOS running on a multicore processor (Figure 1). Coding in high level languages helps a little, but even more so does using an open standards RTOS API like POSIX, and now there are even OS conversion programs that help move applications written for one RTOS API to another. But the porting of the code is just the start. Because embedded systems often have quite stringent and precise system characteristics much of the porting time is spent testing and verifying that the system still operates as required.

So, is there an alternative to moving to an SMP RTOS? A possible alternative is to use an embedded virtualization solution, such as an embedded hypervisor, to help maximize the multiple cores and often other new features of the new generation of multicore processors (such as 64-bit addressing). There are a number of interesting benefits to using virtualization in an embedded system, and the advent of multicore processors really brings some of them to the forefront, especially when compared to using an SMP RTOS.

Virtualization effectively allows users to run multiple operating systems on a single hardware platform, and has been widely used in the enterprise market to run multiple and often different operating systems and their applications on a powerful server platform. This allows the use of legacy operating systems running in virtualized environments on modern hardware platforms that they wouldn't normally be able to run on. On desktop systems virtualization allows users to run multiple different Oses on a single hardware platform, for example running both Windows and MacOS on a Mac.
In the embedded world this same approach can be taken, both to run legacy operating systems, and also to run multiple different operating systems on a single platform. The use of both approaches can lead to some very interesting time and cost savings for embedded developers as they build the next generation of embedded systems using modern multicore processors. First, the virtualization of legacy operating systems can really help the migration of embedded software systems to modern hardware platforms, by providing a ‘virtual’ motherboard with processor, memory and devices presented to the legacy software as if it were a real embedded system.

This approach greatly simplifies a couple of often costly and time consuming tasks in the migration of legacy software. First, an RTOS will usually need to be migrated to a new hardware platform, needing a newer version of the RTOS and usually a new board support package (BSP) to go with it. This can often take significant time and money, and then the applications will need to be moved to and tested on the new version of the RTOS—again a time consuming task. Using virtualization the old version of the RTOS and the applications can be picked up and dropped into the virtual environment, often using virtualized devices to even allow the re-use of the existing BSP, and thus moving straight into more of a testing and verification phase. If we combine this approach with the other virtualization technique of running multiple operating systems on multiple virtual motherboards on a single hardware platform, we can start to unleash the power of multicore processors.

Many embedded system refreshes are done to accommodate feature requirements in the embedded system, maybe more or different connectivity options or a change in GUI. This requires new software to be written and added to the legacy software. This can become quite a challenge if the legacy RTOS has limited connectivity options or dated GUI functionality, and bringing it up to modern standards can be costly. Using virtualization, the legacy software can be left relatively untouched, and housed in its own virtual environment while new functionality can be added in another virtual environment, maybe with a more modern operating system. This can also ensure that the best OS is being used for the different functions in the system, for example using the legacy RTOS for the real-time part of the system and using a more full-featured OS for the networking and GUI aspects. There would need to be a communication mechanism between the operating systems, but this could be relatively simple and is usually well handled by the virtualization software. Each virtual environment could have a dedicated processor core, and in the case of the full featured OS, maybe have more than one physical core dedicated to it to help the processor load of GUI or networking. As there is no processor core sharing between the OSes, the real-time performance of the RTOS won’t be compromised by the full featured OS as it churns through its graphics, network or storage functions.

Another interesting spin-off from this virtualization strategy also helps with the migration from 32-bit to 64-bit, as the embedded applications start to crave the memory and performance that we associate with our modern computers and phones. Running a legacy 32-bit operating system won’t be able to take advantage of the increased memory addressing of a 64-bit processor, even when virtualized. However, running multiple 32-bit OSes on a 64-bit processor will make it possible to allocate the extra addressing in 32-bit chunks, and effectively allow more memory spread over the different virtual machines. This could be a very cost effective way of adding extra functionality and memory usage without having to move to a brand new 64-bit OS.

This is a particularly interesting strategy as we look at certain key embedded processor architectures. The ARM architecture (and specifically the Cortex-A family) has largely been a single-core, 32-bit architecture without hardware virtualization functionality. So, typically one would run 32-bit, non-SMP RTOSes, or variants of Linux and Android, if GPOS functionality is required. Some of the latest processors based on members of the Cortex-A family are now moving to multicore (Cortex A9 for example), or introducing multicore with virtualization support (32-bit Cortex A15 and A7, and 64-bit Cortex A53, A57 and A72). The former case requires a strategy for SMP RTOS, or potentially the use of a hypervisor in the latter case.

Porting the legacy RTOS code to these new multicore Cortex A9 processors could be a tricky undertaking if the legacy RTOS has not introduced a multicore scheduler. This might propel developers to look at using an ARM-based processor that has virtualization support to run the existing 32-bit RTOS in a virtual machine, and add new functionality by adding other operating systems and code in separate virtual machines. This helps preserve the legacy functionality, and allows new features to be added without dramatically affecting the legacy code. It also allows a relatively painless migration from a 32-bit world to a 64-bit world without having to dramatically invest in new RTOSs or new code. In the connected embedded or IoT world...
this is also often an easy way to add new connectivity, by having a VM that specifically looks after the network(s), and the other VM that focuses on the embedded tasks. This not only allows for new network connectivity to be added relatively easily, but also brings in another key factor, the separation of devices.

As discussed earlier, virtualization can provide a number of virtual motherboards, each running their own OS and applications. The devices that are provided in each virtual motherboard can differ from one another and can contain a mixture of virtual or physical devices. As a Memory Management Unit (MMU) on a processor divides up memory and protects the different memory regions for the different applications, an IOMMU does the same for IO devices for different virtual machines. If, for example, you want to have the network device only accessible to the network VM, then you program the IOMMU to restrict network device access to that network VM. The other VMs on the system cannot see or reach the network device, and it doesn't appear on their virtual motherboard. This provides the separation between VMs, and in the world of IoT where the network is the attack vector for cyber threats, the embedded code and data can be protected and separated from those threat points. If, however, you want to have the network shared between different VMs, then you can use the hypervisor to set up virtual devices. The hypervisor controls the physical network interface, and then provides multiple virtual network interfaces to be available on the virtual motherboards as required. Virtualization can therefore provide a very flexible way to split up an embedded system from processor cores, memory and devices and then present them to the ‘guest’ operating systems that are running in the virtual machines.

Figure 2 shows an example where a four-core processor is split into three virtual motherboards. The first virtual motherboard runs an RTOS to run the legacy real-time applications. The second is running a general purpose OS (GPOS), in this case Linux to deal with the networking and storage aspects of the system, and uses the IOMMU to dedicate the networking and storage devices to this GPOS.

The increasing use of multicore embedded processors, especially those offering virtualization support is spurring the embedded world to embrace the use of virtualization. This can provide a very efficient use of the processor cores and devices, help maintain legacy code, and also to help introduce better security into our connected embedded world.

Lynx Software Technologies
San Jose, CA
(408) 979-3900
www.lynx.com

2U server with EXTREME power + cooling

XIOS 2U has:
- Ten slots (PCIeGen2 x8) in a 2U chassis
- 45W per slot with high-volume cooling
- 1-2 Xeon processors
- 1-4 removable disks

See more at edt.com
Microsoft Edge is slated to become the new default web browser for Windows 10, with Internet Explorer consigned to the background to support legacy software. Edge features a host of built-in features such as a screen grab tool with touchscreen doodling abilities, a note pad, and reading mode. Cortana will also be built into the browser.

Another key tweak has been made to one of the most important features of Windows 10, as far as hardcore desktop users are concerned, which is virtual desktops. On previous builds the apps you had open on any desktop were shown on every desktop’s taskbar, making it cluttered. Not so with Windows 10. Multitasking is one of the better executed features in Windows and now Microsoft is adding something it’s calling Task View to make it even more useful. Set on the taskbar at the bottom of the screen, task view, when launched, will display all of your currently opened apps. When you launch task view, Windows 10 will support the ability to view multiple desktops. You can switch between different desktops where multiple apps run. Using the new ‘Snap Assist’ UI you will also be able to grab apps from those different desktops. If it works as advertised, this could be a seriously impressive feature.

Advantech is offering diverse platforms with Windows 10 IoT pre-installed, including boards, systems, and gateways. And Advantech WISE-PaaS Platform as a Service fully supports Windows 10 IoT with Core, Mobile, and Industry versions through Universal Windows Apps structure to offer Cloud Services. By adopting it, developers can rapidly build and deploy applications with greater speed, flexibility, and agility. It enables developers to easily and effectively construct IoT cloud solutions.

Advantech, Irvine, CA
(949) 420-2500. www.advantech.com

Full Support of Microsoft Windows 10
Enabling the IoT

Advantech has announced support of the newly released Windows 10 IoT (Internet of Things). Windows 10 IoT will power a range of intelligent connected devices from smaller equipment such as gateways or mobile point-of-sale units, to industrial devices like robots and specialty medical equipment. Designed to connect through Azure IoT Services, Windows 10 IoT offers enterprise-grade security along with native connectivity for machine-to-machine and machine-to-cloud scenarios.

Azure IoT Suite is an integrated offering that takes advantage of all relevant Azure capabilities to connect devices and other assets (i.e., “things”), capture the diverse and voluminous data they generate, integrate and orchestrate the flow of that data, and manage, analyze, and present it as usable information that either helps people to make better decisions or boosts intelligent automation of operations. The offering, while customizable to fit the unique needs of organizations, will also provide finished applications to speed deployment of common scenarios we see across many industries, such as remote monitoring, asset management and predictive maintenance, while providing the ability to grow and scale solutions to cover millions of “things.”

Within proprietary Windows 10 IoT networks, establishing communication is fairly easy with AllJoyn. AllJoyn is an open source software framework and set of services that aims to enable interoperability among connected devices, regardless of the underlying proprietary technology or communications protocols. By implementing AllJoyn in Windows 10, Microsoft is joining with more than 80 alliance members to support interoperability across a variety of platforms and at scale, advancing the development and vision of IoT.

New Feature Highlights include Cortana, Microsoft’s virtual assistant, which has been present on its phone operating system for a while now, is one of the headline features of Windows 10. Accessible directly from the desktop with either a click or a voice command, it can serve as a handy helper when you need to get things done.

Microsoft Edge is slated to become the new default web browser for Windows 10, with Internet Explorer consigned to the background to support legacy software. Edge features a host of built-in features such as a screen grab tool with touchscreen doodling abilities, a note pad, and reading mode. Cortana will also be built into the browser.

Another key tweak has been made to one of the most important features of Windows 10, as far as hardcore desktop users are concerned, which is virtual desktops. On previous builds the apps you had open on any desktop were shown on every desktop’s taskbar, making it cluttered. Not so with Windows 10. Multitasking is one of the better executed features in Windows and now Microsoft is adding something it’s calling Task View to make it even more useful. Set on the taskbar at the bottom of the screen, task view, when launched, will display all of your currently opened apps. When you launch task view, Windows 10 will support the ability to view multiple desktops. You can switch between different desktops where multiple apps run. Using the new ‘Snap Assist’ UI you will also be able to grab apps from those different desktops. If it works as advertised, this could be a seriously impressive feature.

Advantech is offering diverse platforms with Windows 10 IoT pre-installed, including boards, systems, and gateways. And Advantech WISE-PaaS Platform as a Service fully supports Windows 10 IoT with Core, Mobile, and Industry versions through Universal Windows Apps structure to offer Cloud Services. By adopting it, developers can rapidly build and deploy applications with greater speed, flexibility, and agility. It enables developers to easily and effectively construct IoT cloud solutions.

Advantech, Irvine, CA
(949) 420-2500. www.advantech.com
Low-Power COM Express Compact Modules Offer Pentium and Celeron Processors

A new line COM Express compact module is based on the new Intel Pentium and Celeron processors (codenamed “Braswell”). Based on this new premium class low-power design, the robust TC4A COM Express modules from congatec consume on average just 4 watts while providing increased graphics capabilities and overall performance. Up to 16 graphics execution units can support up to three HD displays or two 4k displays and achieve a theoretical peak performance of 358.4 GFlops per second. Additionally, the widely scalable general processing power - from 1 GHz dual-core to 2 GHz quad-core - prepares the modules for a whole range of fanless and rugged embedded computer designs based on COM Express’ compact footprint.

The conga-TCA4 modules with COM Express type 6 pinout are equipped with the 14 nm Intel Pentium and Celeron processors with a 4 watt SDP (Scenario Design Power) and a 6 watt TDP (Thermal Design Power) plus up to 8 GB of fast dual channel DDR3L 1600 RAM. With the integrated Intel Gen 8 graphics, applications profit from double the graphics performance compared to their predecessors. In addition, support for three independent displays via 2x DP 1.1 or 2x HDMI 1.4b and 1x eDP 1.4 or dual channel LVDS is offered. DirectX11.1 and OpenGL 4.2 ensure a high-quality user experience with the latest 3D features and resolutions of up to 4k (3840 x 2160 @ 30 Hz). The integrated video engine provides jitter-free decoding of H.265/HEVC compressed videos with minimum CPU utilization and encodes two 1080p H.264 video streams at 60 Hz in real-time. As an option, the new modules also simplify innovative, interactive applications with pedestrian recognition and/or gesture control thanks to two onboard MIPI camera interfaces, allowing the direct connection of CSI2 camera sensors.

The new congatec computer modules support the COM Express type 6 pin-out with 5x PCI Express Gen 2.0 Lanes, 1x Gigabit Ethernet, 2x SATA 3.0, 4x USB 3.0, 8x USB 2.0, LPC as well as F/C, UART and HD Audio round off the feature set. Operating system support is offered for all major Linux distributions and variants of Microsoft Windows – including Microsoft Windows 10.

congatec, San Diego, CA
(858) 457-2600. www.congatec.com
**Tool Suite Enhances Visibility into Software Life Cycle**

The version 9.5 release of the LDRA tool suite features new updates that automate manual processes and provide simple, easy-to-use visibility into the relationships between software artifacts at all stages of the software development life cycle from requirements through verification. Used by companies designing safety- and security-critical software in a variety of industries—such as aerospace and defense, medical devices, industrial controls, rail transportation, and automotive—LDRA tool suite 9.5 delivers faster, more effective, time-saving analysis and verification for companies developing critical systems.

Safety-critical systems have become increasingly dependent on software, which has grown dramatically in size and complexity as the speed, memory, and performance of modern systems support additional functionality. As a result, software projects extend across more of an organization and therefore the tools and technologies used to support these efforts are increasingly required to support multiple operating systems and platforms. Linux and all of its variants and dependencies continue to add complexity to the equation. Certifying systems developed and even deployed on these platforms requires software quality and verification tools that can address the need for increased scalability, process automation, and improved visibility into the relationships between software artifacts.

Updates to LDRA tool suite 9.5 tackle these challenges head on. Simplified, automated processes have streamlined how users create test cases while a clearer, expansive "Uniview" of the software components and artifacts improves understanding of requirement traceability, system interdependency and behavior, and overall standards compliance objectives. Enhanced Linux support automates dependency checking, greatly simplifying and speeding up the analysis of code in these environments. With the 9.5 release, users also have the ability to add custom attributes and types kept with each requirement or test case enabling the product to be customized and tuned to various project requirements for information and record keeping.

The LDRA tool suite offers independent verification support across the full development life cycle from certification objectives of standards, such as DO-178C, ISO 26262, IEC 61508, EN 50128, and IEC 62304, to requirements, code, and target testing.

**Security Management for IoT, Industrial Control, Medical, Smart Grid and DoD Devices**

A security management software suite that is specifically designed to protect IoT and embedded devices against cyber-attack can be operated as either an on-premise or a cloud-based security manager. The Floodgate Security Manager from Icon Labs provides device status monitoring, security policy management, command audit logging, and security event logging and reporting for devices running Icon Labs’ Floodgate Agent or other lightweight IoT management protocols such as COAP and MQTT. Floodgate Security Manager provides comprehensive reporting and auditing capabilities to help achieve ESDA Certification, ISA/IEC 62443 Compliance, and/or compliance with the NIST Cybersecurity framework.

The current approach to security management for IoT devices is to repurpose legacy security management systems. While this solution works for some IoT gateways and other large IoT devices, it does not scale to the smallest IoT devices, especially small battery powered edge devices and sensor solutions. Floodgate Security Manager is designed to provide the management services required by all IoT devices, including small, battery powered and mobile devices without the overhead and complexity of traditional enterprise security management systems.

Icon Labs products provide embedded security for IoT and Machine to Machine (M2M) solutions such as aerospace, military and space probes, industrial and medical control devices, medical systems, and consumer electronics products. The Floodgate Security Framework provides a "defense in depth" solution that protects control units and endpoint devices from cyber threats, aids in compliance with regulatory mandates and guidelines, and gathers and reports command, event and device status information for audit requirements.

**Icon Laboratories, Des Moines, IA**
(515) 226-3443. www.iconlabs.com

**LDRA, Atlanta, GA**
(855) 855-5372. www.ldra.com
In-Vehicle Electronics Protected in Rugged IP65-rated Box PC

A new IP65-rated, maintenance-free box computer is suitable for data acquisition in extreme environments throughout a number of in-vehicle applications, such as trains, commercial vehicles, mobile machines and ships. On the BC50R from MEN Micro, all external interfaces, including USB, digital I/O, Gigabit Ethernet, CAN bus and legacy serial I/O, are implemented on rugged M12 connectors for reliable data transmission. Offering a protection class of IP65, the new box computer is certifiable to EN 50155 (railway) or EN 60945 (shipping) and conforms to ISO 7637-2 (E-mark for automotive).

The BC50R starts with a powerful, energy-efficient T48N AMD Embedded G-Series APU running at 1.4 GHz. Various CPU/GPU options combine with a wide selection of external interfaces, connected via separate graphics and I/O interface boards within the system, to provide an extremely flexible system quickly tailored to a vast number of applications.

Inside the system, two PCI Express Mini card slots with two SIM card slots offer WLAN, GPS, other GNSS or 3G/4G functionality. The necessary antenna connectors can be made available at the front panel. The BC50R is equipped with 2 GB of DDR3 SDRAM and offers SD card and mSATA slots. Additional memory resources include 64 KB of L1 cache and 512 KB of L2 cache. An extremely robust aluminum housing protects the internal electronics, and the system’s fanless design operates at temperatures from -40°C to +70°C (+85°C for up to 10 minutes).

The new box PC supports either a 24 VDC and 36 VDC nom. (10 V to 50.4 V) class S2 power supply in compliance with EN 50155 or power supplies with a nominal input voltage of 24 V that either comply with ISO 7637-2 or EN 60945.

MEN Micro, Blue Bell, PA
(215) 542-9575. www.menmicro.com

Low-Power Small-Form-Factor PCIe-Based SSDs for Embedded, Industrial Designs

A new family of PCI Express (PCIe)-based SSDs features small size and power requirements under four watts, making them attractive storage solutions in space- and air-restricted embedded/industrial applications. The new Virtium StorFly SSDs, available in both M.2 and Mini Card form factors, are specifically designed to operate at low power and offer highly reliable and compatible drop-in storage for systems at the center of communications, networking, data acquisition, automation, and other demanding applications.

Drawing less power allows the new Virtium SSDs to generate less heat – higher temperatures diminish storage performance – which improves the devices’ reliability in systems where space is limited and airflow minimal, if not absent entirely. The M.2 and Mini Card drives’ value to these environments is further enhanced by their small “footprints” – 22x80mm for M.2, 30x51mm for Mini Card. The combined low power and small size provides system designers with the capability to scale their capacity by allowing integration of multiple SSDs all within a limited power budget or system footprint.

Built on Virtium’s established and widely deployed StorFly platform, the new M.2 and Mini Card SSDs are available in capacities of 16GB, 32GB, 64GB, 120GB, 240GB, and 480GB. SSDs in this range are targeted for when reliability and compatibility take priority over capacity – such as in boot drives, data logging and read-oriented solutions -- and provide system designers with more cost-efficient storage options. The M.2 and Mini Card drives’ PCIe 2.0 interface provides a future-proof solution as it enables access to a growing ecosystem of processors, systems and software developed around PCIe.

Virtium, Rancho Santa Margarita, CA
(949) 888.2444. www.virtium.com
Wind River Drives IoT Device Development with Real-Time Virtualization Offering

Wind River has announced a major update to its real-time virtualization offering that allows customers to further reduce cost and innovate connected devices. The update includes storage virtualization capabilities, enhanced security capabilities, and expanded processor support.

Virtualization Profile for VxWorks is based on Wind River virtualization technology and extends the scalability capabilities of VxWorks by integrating a real-time embedded, Type 1 hypervisor into the core of the real-time operating system (RTOS). Through embedded virtualization, it allows VxWorks customers to consolidate multiple disparate workloads on a single processor. Critical in today’s era of IoT, it helps to address the need for robust, safer and more secure partitioning across all market segments.

“Virtualization is a key attribute in GE’s global vision for industrial control systems in the era of the Industrial Internet. It allows the GE businesses to combine their real-time control logic, HMI, security, and cloud connectivity into a single platform,” said Wes Skeffington, principal engineer at GE. “Wind River’s virtualization offering provides the right attributes like scalability, storage virtualization, real-time behavior, virtual machine isolation, and security capabilities to realize this vision.”

Updates to Virtualization Profile for VxWorks include storage virtualization through VirtIO allows devices to share a single storage controller, even a single disk, such as a Serial ATA device between multiple virtual machines (VMs), thereby dramatically reducing cost and complexity for consolidated systems. The run-time configuration, combined with support for the VirtIO device virtualization framework makes the virtualization profile a flexible and highly customizable virtualization layer for embedded devices.

Wind River, Alameda, CA
(510) 748-4100. www.windriver.com

Flexible Dual-Mode Bluetooth Module Accelerates Development

A dual-mode Bluetooth Smart Ready module solution gives embedded developers great flexibility to integrate both Bluetooth Smart and Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR) wireless technologies while minimizing design time, cost and complexity. The new Bluetooth Smart Ready BT121 module from Bluegiga, a Silicon Labs company, provides a pre-certified, fully integrated, high-performance solution that includes the Bluetooth radio, microcontroller (MCU) and on-board Bluetooth software stack supported by Silicon Labs’ complimentary Bluetooth Smart Ready software development kit (SDK) and easy-to-use BGScript scripting language.

The BT121 Bluetooth Smart Ready module and software are designed to help developers accelerate time to market and reduce development costs and compliance risks by providing a versatile, plug-and-play Bluetooth solution. The BT121 module is suitable for applications requiring connectivity to legacy devices that only support Bluetooth BR/EDR, as well the latest applications using Bluetooth Smart such as connected home, health and fitness, wearables and point-of-sale terminals. There are millions of legacy smart phones, tablets and PCs still in service that do not support Bluetooth Smart technology. Additionally, some applications require the higher throughput advantages of Bluetooth Classic technology, which Bluetooth Smart is not designed to achieve.

The BT121 module provides a “best of both worlds” solution for both ultra-low-power and high-data-rate Bluetooth connectivity applications. The module can connect to legacy devices that only support Bluetooth SPP or Apple iAP2 profiles, for example, as well as to devices that support Bluetooth Smart. The easy-to-use BT121 module integrates a high-performance Bluetooth radio with an extended range of up to 400 meters, a low-power ARM MCU, and a fully certified Bluetooth Smart Ready protocol stack in a compact 11 mm x 14 mm surface-mount package, making this one of the smallest Bluetooth Smart Ready modules in the market.

No RF or Bluetooth protocol development expertise is necessary to implement the BT121 module in Bluetooth designs. The module can be used as a peripheral along with an external host MCU, or applications can be embedded into the built-in MCU with the Bluegiga BGScript scripting language, creating a completely standalone design with minimal external components.

Silicon Labs, Austin, TX
(512) 416-8500. www.silabs.com
## ADVERTISER INDEX

GET CONNECTED WITH INTELLIGENT SYSTEMS SOURCE AND PURCHASABLE SOLUTIONS NOW

Intelligent Systems Source is a new resource that gives you the power to compare, review and even purchase embedded computing products intelligently. To help you research SBCs, SOMs, COMs, Systems, or I/O boards, the Intelligent Systems Source website provides products, articles, and whitepapers from industry leading manufacturers—and it's even connected to the top 5 distributors. Go to Intelligent Systems Source now so you can start to locate, compare, and purchase the correct product for your needs.

![Image of RTC Magazine](RTC_magazine.png)

<table>
<thead>
<tr>
<th>Company</th>
<th>Page</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acromag</td>
<td>32</td>
<td>acromag.com</td>
</tr>
<tr>
<td>Artila</td>
<td>21</td>
<td>artila.com</td>
</tr>
<tr>
<td>Avnet</td>
<td>2</td>
<td>em.avnet.com</td>
</tr>
<tr>
<td>congatec, Inc.</td>
<td>4, 17</td>
<td><a href="http://www.congatec.us">www.congatec.us</a></td>
</tr>
<tr>
<td>Dolphin Interconnect Solutions</td>
<td>29</td>
<td>dolphinics.com</td>
</tr>
<tr>
<td>EDT</td>
<td>44</td>
<td>edt.com</td>
</tr>
<tr>
<td>Infineon</td>
<td>33</td>
<td>infineon.com</td>
</tr>
<tr>
<td>Intelligent Systems Source</td>
<td>9</td>
<td><a href="http://www.intelligentsystemssource.com">www.intelligentsystemssource.com</a></td>
</tr>
<tr>
<td>Lauterbach</td>
<td>50</td>
<td>lauterbach.com</td>
</tr>
<tr>
<td>MPL</td>
<td>4</td>
<td>mpl.ch</td>
</tr>
<tr>
<td>One Stop Systems</td>
<td>12, 37</td>
<td><a href="http://www.onestopystems.com">www.onestopystems.com</a></td>
</tr>
<tr>
<td>Portwell</td>
<td>52</td>
<td>portwell.com</td>
</tr>
<tr>
<td>RTECC</td>
<td>50</td>
<td>rtecc.com</td>
</tr>
<tr>
<td>Super Micro Computers, Inc.</td>
<td>13</td>
<td>supermicro.com</td>
</tr>
<tr>
<td>Trenton Systems</td>
<td>51</td>
<td><a href="http://www.TrentonSystems.com">www.TrentonSystems.com</a></td>
</tr>
<tr>
<td>WinSystems</td>
<td>5</td>
<td>WinSystems.com</td>
</tr>
<tr>
<td>Product Gallery</td>
<td>41</td>
<td></td>
</tr>
</tbody>
</table>
Rugged Made in America
Computer Built For Performance

Trenton Systems®
Engineered For Reliability

Trenton wrote the book on powering application ready platforms with long-life, Made in America core computing technology and backplane infrastructure. Our rugged system design approach gives you the flexibility to mix and match industry standard COTS plug-in cards to precisely match the job requirements. Designing and manufacturing SBCs and backplanes in America results in systems that maximize hardware security and computing performance.

Trenton Systems’ Made in America application ready platforms features include:

- Robust, long-life, dual-processor system host boards
- Flexible system backplane and device I/O configurations
- Secure PCIe 3.0 link expansion using standard plug-in cards

To learn more about our latest application ready platforms visit www.TrentonSystems.com or give us a call at 770.287.3100, or toll free in the United States at 800.875.6031

The Global Leader in Customer Driven Computing Solutions™

Made in USA

IoT Solutions Alliance
Portwell Empowers Intelligent Solutions

Mini-ITX

Small Form Factor System

COM Express Module

Network Security Appliance

PICMG SBC