EMBEDDED SYSTEMS ENGINEERING powered by EECatalog

Engineers' Guide to IoT and M2M

Europe's Take on the IoT

The Internet of Things

Embedded Memories Destined for IoT Seek Security/Power Management Balance

The IoT and RTOS Reinvention

www.eecatalog.com/IoT

We simplify the use of embedded technology

FAST AND COMPACT
conga-TC97

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

HIGH END PERFORMANCE
conga-TS87

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

POWERFUL AND SMALL
conga-MA3/conga-MA3E

- COM Express Mini Type 10 module
- Intel® Atom™ and Intel® Celeron® processors
- Gen 7 Intel® HD graphics
- Extended temperature range option

HIGH PERFORMANCE QSEVEN
conga-QA3

- Qseven module
- Intel® Atom™ and Intel® Celeron® processors
- Gen 7 Intel® HD graphics
- Extended temperature range option

Find more details at: **www.congatec.us**

congatec Inc. | 6262 Ferris Square San Diego | CA 92121 USA |
Phone: 858-457-2600 | sales-us@congatec.com

intel IoT Solutions Alliance

congatec

Toradex
Embedded. Computing.

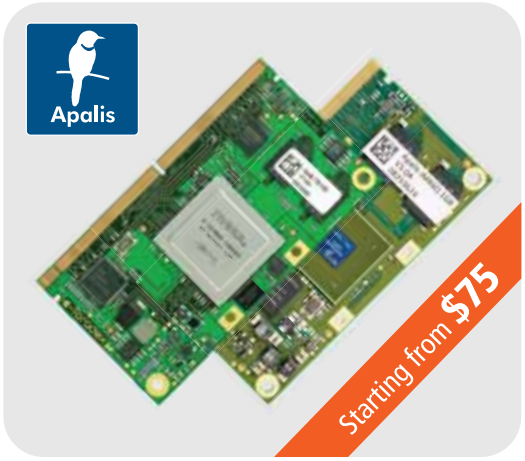
500+ Million People rely on Toradex everyday

Free Premium Support

Local Warehouses

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

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



High Performance

Low Power

Fast Boot

Direct Support

Extensive Ecosystem

Long Lifecycle

Toradex Inc. I 219 1st Ave S, Suite 410 I Seattle, WA 98104 I USA I seattle@toradex.com T: +1 (800) 871-6550

CONTENTS

Engineers' Guide to IoT and M2M

Features

Product Showcases

Engineers' Guide to IoT and M2M
www.eecatalog.com/IoT

Vice President & Publisher
Clair Bright

Editorial
Editor-in-Chief
Chris Ciufo
cciufo@extensionmedia.com
Managing Editor
Anne Fisher
afisher@extensionmedia.com
Contributing Editor
Caroline Hayes

Creative/Production
Production Manager
Spryte Heithecker
Graphic Designers
Nicky Jacobson
Caldin Seides
Media Coordinator
Yishian Yao
Senior Web Developers
Slava Dotsenko
Mariam Moattari

Advertising / Reprint Sales
Vice President, Sales
Embedded Electronics Media Group
Clair Bright
cbright@extensionmedia.com
(415) 255-0390 ext. 15
Sales Manager
Michael Cloward
mcloward@extensionmedia.com
(415) 255-0390 ext. 17
Marketing/Circulation
Jenna Johnson

To Subscribe
www.eecatalog.com

Extension MEDIA

Extension Media, LLC Corporate Office
President and Publisher
Vince Ridley
vridley@extensionmedia.com
(415) 255-0390 ext. 18
Vice President & Publisher
Clair Bright
cbright@extensionmedia.com
Vice President, Business Development
Melissa Sterling
msterling@extensionmedia.com
Human Resources / Administration
Rachael Evans

Special Thanks to Our Sponsors

INTERNET OF THINGS DEVELOPERS CONFERENCE

May 6-7, 2015
Hyatt Regency Santa Clara, CA

Resolving the Technical and Business Challenges of Getting Connected to the Internet of Things

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

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

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

IoT-devcon.com

Europe's Take on the IoT

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

By Caroline Hayes, Senior Editor

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

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

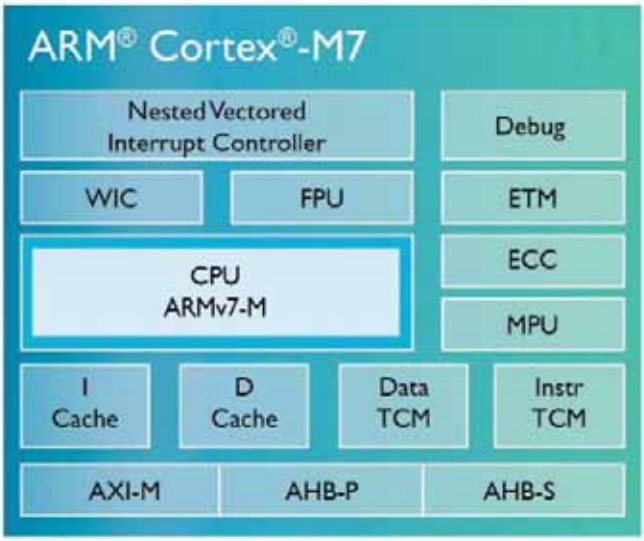


Figure 1: The ARM® Cortex®-M7 provides the means to boost performance and capability for embedded IoT processors.

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

ONTO INTERNET 2025

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

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

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

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

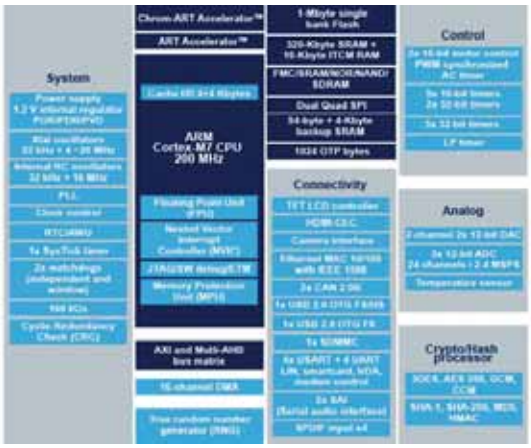


Figure 2: STMicroelectronics' STM32 F7 is based on the ARM® Cortex®-M7 core.

the deep-sleep RAM and quick wake-up modes will keep information dynamic, he adds.

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

POWER CONCERNS

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

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

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

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

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

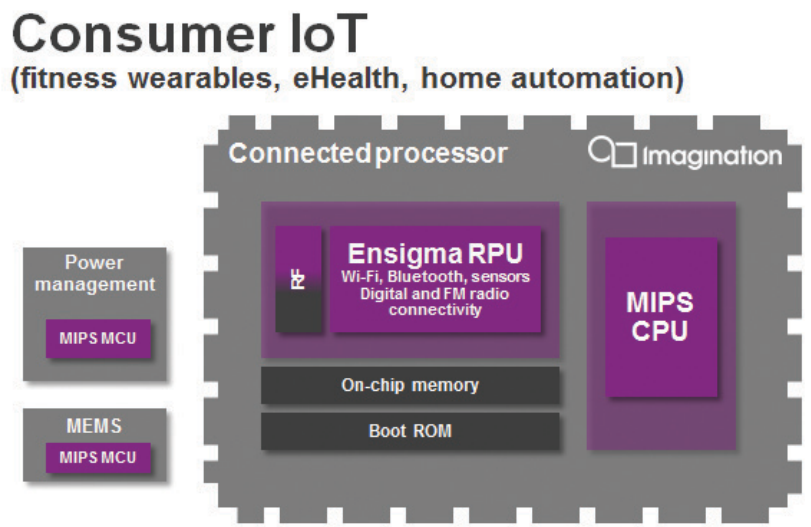


Figure 3: Imagination Technologies focuses on low power consumption to provide consumer IoT embedded designs.

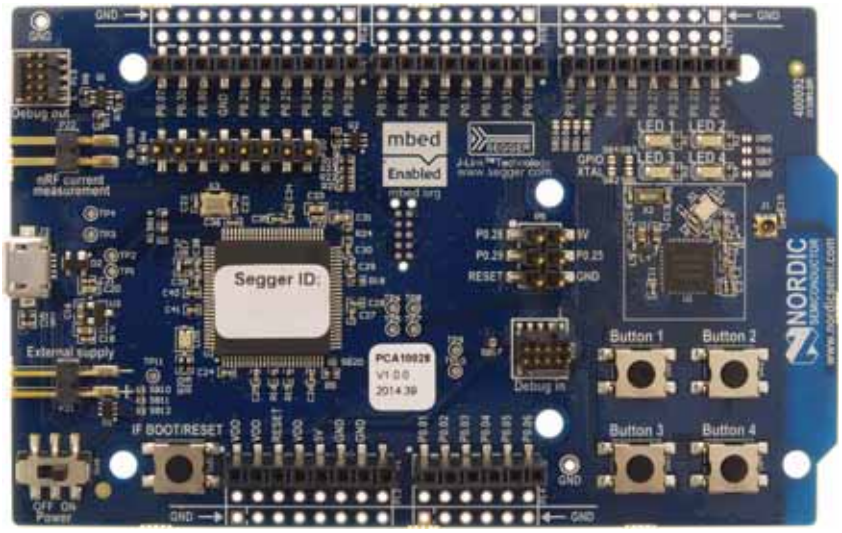


Figure 4: An Arduino Uno, shield-compatible, single board development kit from Nordic Semiconductor supports ARM® mbed™ for rapid prototyping of wireless designs.

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

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

Vendor Spotlight: VDC Research on ADLINK

ADLINK TECHNOLOGY INC.
HQ: 9F, No.166 Jian Yi Road | Zhonghe District New Taipei City 235, Taiwan
Founded: *1995*
Funding/Key Investors: *ADLINK Technology is a public company listed as 6166 on TAIEX*
Number of Employees: *1,456*
Contact: *www.adlinktech.com*
info@adlinktech.com

COMPANY BACKGROUND

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

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

BUSINESS MODEL

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

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

PRODUCT PORTFOLIO AND TECHNICAL CAPABILITIES

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

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

ADLINK's Smart Embedded Management Agent (SEMA), which comes supported by the majority of board and system products equipped with a board management controller, enables monitoring and collection of systems performance and status information from the embedded hardware. The SEMA-cloud solution pushes system data to the data center server through any kind of TCP/IP connection – ultimately enabling easier access to data and analytics through any commercial cloud portal. ADLINK selected Gemalto in May 2014 as their partner to complete the cloud integration, enabling remote system monitoring and real-time maintenance for connected devices using SEMA via a secure web-based dashboard.

ADLINK also offers industrial mobile computing products such as Smart Panels, rugged tablets, and handheld mobile computers supporting Android and Windows operating systems. The company's COM products span a variety of architectures such as COM Express, SMARC, Qseven, and ETX. By supplying a flexible product portfolio for OEMs to easily augment their designs with a variety of peripherals and functionality, OEMs can focus on differentiating their products and reducing time-to-market. The company also supplies a variety of other embedded computing products such as slot SBCs and carriers, ATCA boards, CompactPCI boards, VPX blades, embedded flash storage, chassis, and more.

SERVICE AND SUPPORT

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

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

COMPETITIVE POSITIONING

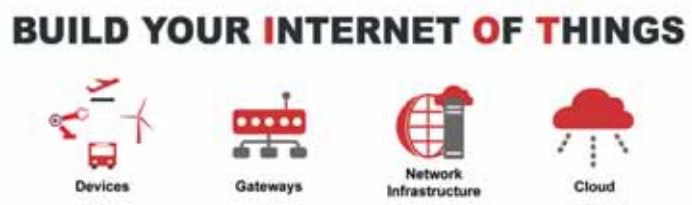
ADLINK is a market share leader in a variety of embedded hardware markets such as embedded motherboards, SBCs, COMs, and embedded integrated computer systems. Combined with its data acquisition experience, products, and resources, the company is able to satisfy a broad range of IoT requirements while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

The industrial automation, medical, and transportation markets present the greatest near-term opportunities for ADLINK, as the company's embedded products and rugged devices are suitable for a variety of field applications within these industries. Further, the company's data acquisition experience will help ADLINK absorb some share from larger competitors such as Advantech and Kontron in these markets and the instrumentation sector, all of which require progressively greater data management to accommodate IoT data streams.

VDC RESEARCH OPINION

ADLINK is positioned to be a premier partner and provider for enabling IoT services and solutions for a variety of ecosystem players over the next several years. The company is reputable in having supported deployments in more than 40 countries across five continents for several different tier-1 OEMs. ADLINK sees the growing value proposition of an integrated product portfolio spanning hardware, software, and (cloud) services, and realizes that this level of IoT enablement is not completely met by its larger competitors in the traditional embedded space.

However, ADLINK is still smaller in size than some of its competitors in the embedded space such as Advantech, Emerson, and Kontron. Competitors such as Eurotech have already brought embedded devices supporting M2M cloud infrastructures to market. Nevertheless, ADLINK can adapt more quickly to changes in market conditions and end user preferences (e.g. wired/wireless protocol/application support, form factor use, etc.). The company also continues to make dramatic steps in building its support for cloud-based deployments and facilitating the engineering of connected devices/infrastructure. When OEMs and other embedded hardware consumers make a purchasing decision, they are typically investing into a multiyear relationship and dependency of a supplier. ADLINK's double-digit revenue CAGR through the last decade, strong profitability, and solid relative growth among its competitors make it a prime candidate as a partner and provider of embedded technology.



Making the Transition to 4G LTE

WHY THE TRANSITION TO 4G LTE?

AT&T will be shutting down the 2G GSM network on January 1, 2017, forcing the machine-to-machine (M2M) industry to begin transitioning to 2G CDMA, 3G HSPA, or 4G LTE networks. This represents a major challenge for the M2M industry, as it will entail the replacement of devices, new contracts with network carriers, and time and cost of major system-wide changes. At first glance it may seem like the GSM carriers just don't want to keep supporting the old 2G networks, so you may be wondering why that is. The answer is quite simple: they are running out of frequencies. Each carrier in the US is only allotted a certain band of the cellular frequency spectrum, and with the high data rate demands of 4G it uses many more frequency bands than the previous 2G and 3G standards. So if some of these frequencies are reserved for "2G only" signals, then they don't have enough bandwidth left for the 4G network. This part is the stick, the carrot part of the 4G transition is because the 4G protocol is much more efficient at combining both voice and data. With 2G and 3G, voice and data travels across different paths in the network, so there is no way to share capacity between these two paths. However with 4G, both voice and data are sent across the same path in the network, so carriers can easily optimize their networks to get the best possible utilization of their bandwidth.

BENEFITS OF 4G LTE

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

WHAT THIS MEANS FOR THE M2M INDUSTRY

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

4G LTE ANTENNA CONSIDERATIONS

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

4G LTE CERTIFICATION

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

SYMMETRY'S 4G LTE SOLUTIONS

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

Symmetry offers replacements for existing 2G GSM design-ins. Multitech offers a number of M2M products covering 2G CDMA, 3G HSPA, and/or 4G LTE, including the embedded SocketModem Cell, the embedded SocketModem iCell, the MultiConnect® rCell 100 Series, the MultiConnect® Cell 100 Series, and the QuickCarrier™ USB-D dongle.

Symmetry also offers exclusive custom Telit IN-A-BOX kits for 3G HSPA and 4G LTE connectivity. These kits are designed to make cellular M2M design easier by providing development kits based on the Telit CE910, DE910, HE910 and GE864-GPS M2M modules. Each kit includes everything required to begin a cellular design for a variety of applications: a Telit EVK2, a Telit Interface Board, software development introduction tools, cellular antenna(s), power supply, and the Getting Started Guide and documentation.

Call Symmetry Electronics at (310) 536-6190 for technical guidance and all the latest M2M connectivity devices.

CONTACT INFORMATION

SYMMETRY ELECTRONICS CORPORATION

Symmetry Electronics Corp.

www.SymmetryElectronics.com

Embedded Memories Destined for IoT Seek Security/Power Management Balance

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

By Bernd Stamme, Kilopass Technology

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

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

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

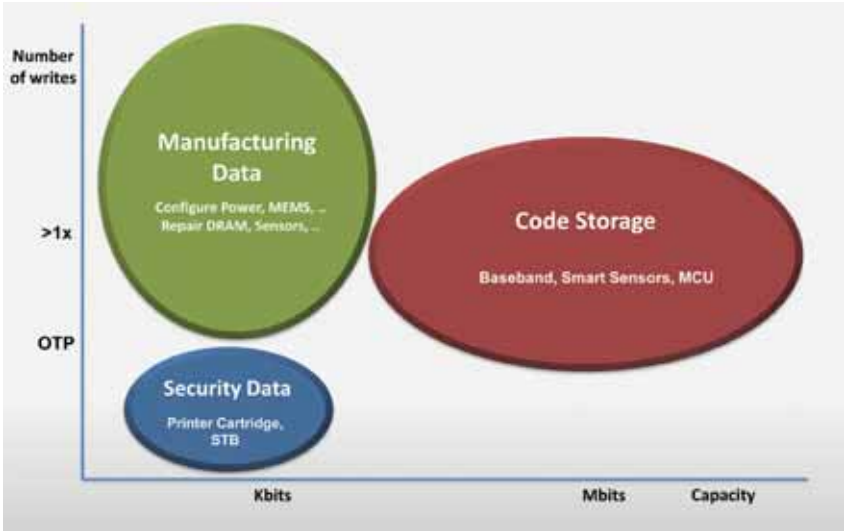


Figure 1: An embedded NVM memory IP is used in a variety of chips for secure storage.

PROTECTION AT THE MOST VULNERABLE LAYER

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

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

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

impenetrable to all but organizations not constrained by normal funding or time considerations.

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

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

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

The IoT and RTOS Reinvention

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

By Thom Denholm, Datalight

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

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

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

DISTRIBUTION MODEL EMULATES IOT APPROACH

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

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

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

MORE RAPID INTEGRATION

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

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

through a full suite of customized attributes, in a fashion similar to recent Linux offerings.

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

One key market for secure devices is medical, and we believe this sector's demands can be well served by a set of offerings from Wind River and Datalight that spans the time and space partitioning scheduler to cryptography libraries and extends from Wind River's secure sockets to the complete protection from power interruption Datalight software offers.

The reasons noted here are why we at Datalight are excited about this new Wind River release, and we're convinced the protected boot, signed images and other security options are exactly where embedded devices need to be. Modularizing the kernel means fewer "complete system" upgrades and more flexibility for OEMs and BSPs. We're pleased to continue supporting Wind River VxWorks with our reliable data storage products.

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

Reconfigurable Image Sensors Make Imagination the only Limit for Innovative IoT Use

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

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

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

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

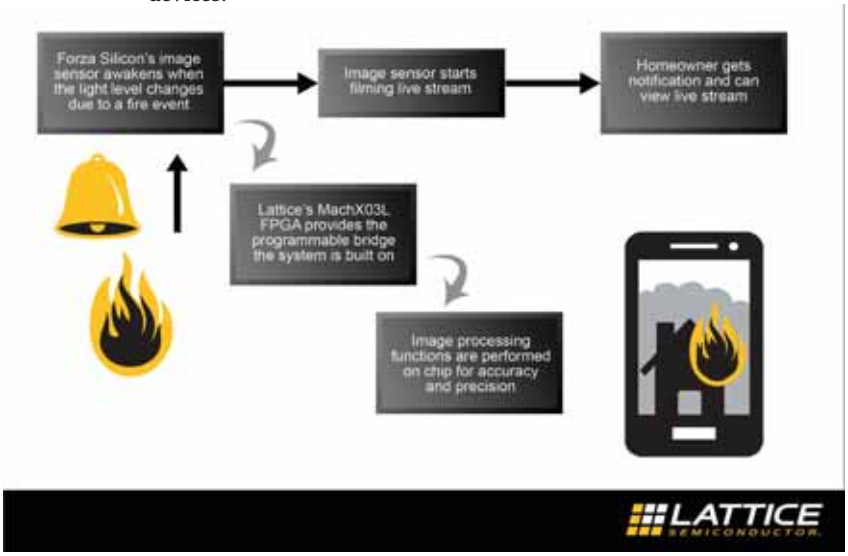


Figure 1. An Internet-connected smoke detector device.

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

BEYOND SMOKE DETECTION

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

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

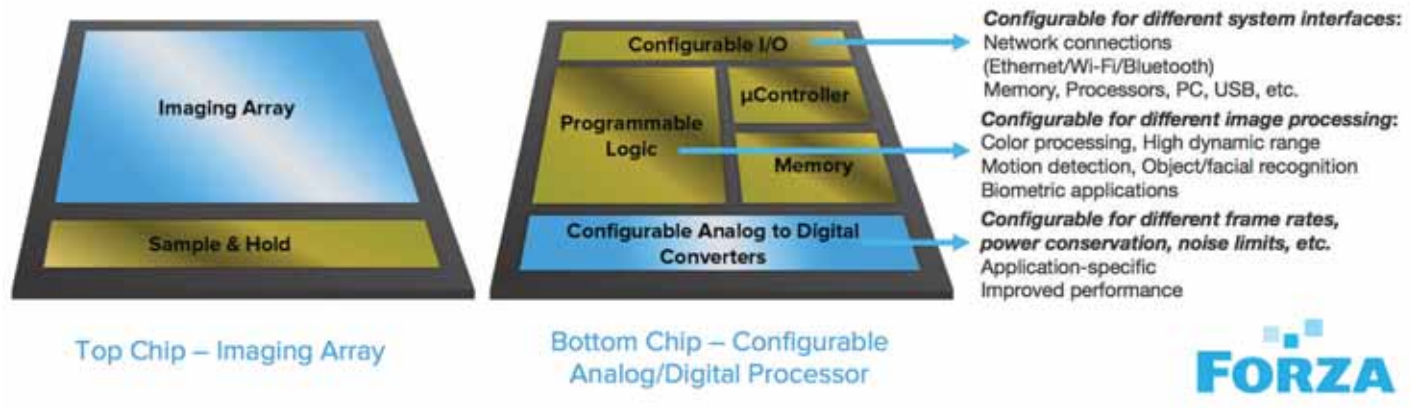


Figure 2. Consumers and businesses could see the imaging possibilities for IoT devices greatly expand thanks to strides made in the fields of sensors and programmable logic.

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

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

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

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

Securing Embedded Devices In The IoT Era

In this corner, a deeply embedded device with limited resources. In the other, pervasive determination to exploit connectivity for the purpose of getting up to no good.

By Daniela Previtali, Wibu-Systems and Michael Weinstein, Wind River

In a recent study, Spanish security researchers reported that smart meters installed by a utility in Spain to meet government energy efficiency goals lacked basic safeguards, leaving room for hackers to carry out billing fraud or even cause blackouts. Weak encryption used in these smart meters allowed the researchers to get hold of the encryption keys used to scramble all the information that the smart meter shares with "nodes" sitting higher in the power distribution system. Using the keys and the unique identifier associated with each meter the researchers were able to spoof messages being sent from the power-watching device to a utility company and make the smart meter under-report the energy use. Shared IDs, poor protection against tampering and data formats that would be easy to fake have been identified as problems for smart meters deployed in other countries, such as the US and the UK, too.

Just in 2014, multiple data breaches at JPMorgan Chase, Home Depot, Albertsons and others compromised in excess of 150 million accounts in the US alone. Piracy and reverse engineering of embedded devices and software also remain a big issue that costs embedded device vendor billions in lost revenues. A German Engineering Federation (VDMA) study indicates that 9 in 10 companies with over 500 employees are affected by piracy that caused €7.9 billion in losses for the German economy in 2013 alone. In 51 percent of the cases, the complete machine was subject to plagiarism.

Clearly, the importance of connected embedded systems being impermeable to cyber-attacks, acts of industrial sabotage and data theft has become paramount. But how can one safeguard deeply embedded endpoint devices that usually have a very specific, defined mission with limited resources available to accomplish it? Embedded devices are designed for low power consumption, with a small silicon form factor, and often have limited connectivity options. They typically have only as much processing capacity and memory as needed for their tasks. And they are often "headless"—that is, there isn't a human being operating them who can input authentication credentials or decide whether an application should be trusted; they must make their own judgments and decisions about whether to accept a command or execute a task. For example:

In factory floor automation, deeply embedded programmable logic controllers (PLCs) that operate robotic systems are typically integrated with the enterprise IT infrastructure. How can those PLCs be shielded from human interference while at the same time protecting the investment in the IT infrastructure and leveraging the security controls available?

Similarly, control systems for nuclear reactors are attached to infrastructure. How can they receive software updates or security patches in a timely manner without impairing functional safety or incurring significant recertification costs every time a patch is rolled out?

IoT sensor hubs aggregate a representative data set from numerous packets of sensed data. How can these real-time operating system (RTOS)-based devices open those packets, validate their integrity, analyze their contents and verify that these actions have taken place securely without compromising the speed and performance5?

The answer is in designing systems for security from the start and incorporating a comprehensive set of security features to efficiently and effectively protect devices and data throughout their lifecycle.

DESIGNING FOR SECURITY

Security cannot be thought of as an add-on to a device, but rather as integral to the device's reliable functioning. Software security controls need to be introduced at the operating system level, take advantage of the hardware security capabilities now entering the market, and extend up through the device stack to continuously maintain the trusted computing base.

Building security in at the OS level is critical, since adding it at the user or application level is ineffective, expen¬sive and risky. Enabling security at the OS level can also take the onus off device designers and developers to configure systems to mitigate threats and ensure their platforms are safe.

PROTECTING DEVICES AT EVERY STAGE

Security must be addressed at every stage—from boot-up to operation to data transmission to

powering down (Figure 1). Being able to add hardware-based security to software-only features can help significantly harden device security overall.

SECURE BOOT

When power is first introduced to the device, the authenticity and integrity of the software on the device must be verified using cryptographically generated digital signatures to prevent the injection and execution of malicious code. In much the same way that a person signs a check or a legal document, a digital signature attached to the software image and verified by the device ensures that only the software that has been authorized to run on that device, and signed by the entity that authorized it, will be loaded. Binaries must be verified at every stage of the boot-up process. If a component fails to pass signature verification, boot must stop.

RUNTIME SECURITY

With Secure Boot, the foundation of trust has been established, but the device still needs protection from various run-time threats and malicious intentions. Preventing unauthorized execution and other forms of tampering with system code is a critical component for securing devices in operation. A solution that can decrypt (using AES or other encryption) and verify digital signatures (using Elliptic Curve Cryptography (ECC), for example) of downloadable kernel modules and real-time processes can effectively protect the integrity of the system and safeguard intellectual property from piracy and code from reverse engineering.

ACCESS CONTROL

User management features are required to safeguard devices from unauthorized access and enable the definition and enforcement of user-based policies and permissions, implementing restrictions and controlling access to the device based on user credentials.

NETWORK SECURITY

It is critical for a connected device to incorporate features to effectively secure network communications using technologies such as SSL (Secure Sockets Layer protocol), SSH (Secure Shell protocol), IPsec and IKE.

DATA PROTECTION

Technologies such as encrypted containers can help safeguard data when the device is powered down, as data in containers remain encrypted even when the device is idle or powered off.

SECURITY AND PERFORMANCE IN BALANCE

In today's demanding market, a controller must not only deliver maximum performance, but also provide seamlessly integrated security. Strict security policies and potent firewalls prevent unauthorized intrusions. Communications and data exchange are subject to additional scrutiny through separate processes. However, the control of a smart plant needs to go beyond this traditional paradigm and offer new security features well suited to harsh environments, and fully reliable for industrial processes.

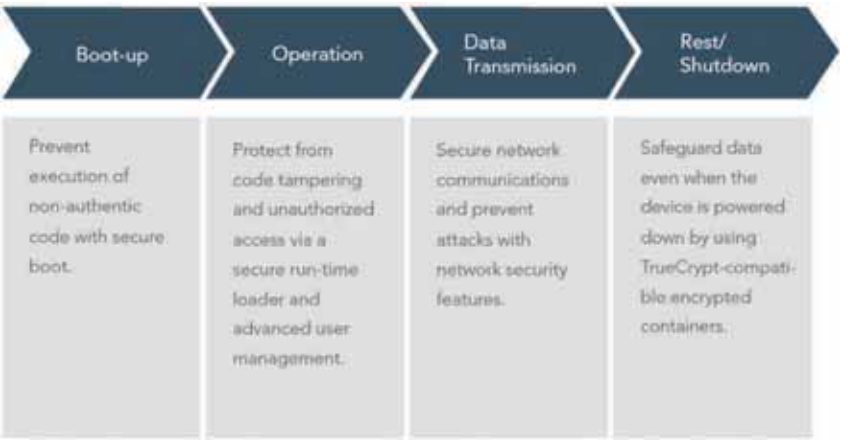


Figure 1: Security throughout the embedded devices' lifecycle.

Let's imagine a European power grid vendor that develops its own PPC-based controller running VxWorks. The production of such hardware, including the download and testing of the related firmware, would be carried out in China. It becomes mission critical to transfer the license from the vendor headquarters to the production facility through a secure channel, and maintain full control over the workflow.

The vendor can easily attain protection against know-how piracy, reverse engineering and tampering, by introducing Security Profile and CodeMeter Security. In particular, IP protection would be achieved through the combined use of CodeMeter and the Secure ELF Loader from Wind River and Wibu-Systems. Reverse engineering protection would be ensured by CodeMeter high encryption standards, which would make it impossible to analyze the cyphered firmware. Copy protection would be the result of CmActLicense, the soft license container bound to a secure element on the embedded system. Tamper protection would be reached through code signing operated by authorized team members only, secure boot and signature verification performed by the Secure ELF Loader in VxWorks. The staff would in fact own CmDongles, in the form of CmStick for USB ports and CmCards for SD slots; the private key would then be securely stored in the smart card chip, the dongles would be configured for use with a password, and set to expire after a predetermined time.

The return in investment stems not just from ensuring optimal security standards, but also from redesigning the licensing blueprint, and introducing scalable business models based on logistic efficiency and feature on-demand dynamics, which could be realized with the Secure ELF Loader and CmActLicense.

A SAFE AND SECURE RTOS FOR IOT

Powering billions of embedded devices, VxWorks® is the world's most widely deployed real-time operating system. Enhanced by Security Profile for VxWorks, the RTOS provides a comprehensive set of software-based security features that enable manufacturers of intelligent embedded devices deliver cutting-edge, rock-solid security in their products. The expandable, upgradable architecture of VxWorks separates the core kernel from middleware, applications, and other packages, enabling bug fixes, upgrades, and new feature additions to be performed as frequently as necessary and without disrupting other technologies in an installation.

Security Profile for VxWorks is a readily expandable solution that can be enhanced with Wibu-Systems' CodeMeter® hardware-based security to enable a comprehensive solution for security-sensitive applications. With software and hardware components as well as activation-based licensing, the joint solution delivers an optimal way to protect devices, data and IP in the Internet of Things.

Daniela Previtali is a Global Marketing Manager at Wibu-Systems, responsible for both corporate and channel marketing strategy and activities.

Michael Weinstein is Senior Product Marketing Manager at Wind River driving the product marketing efforts pertaining to the VxWorks real-time operating system and the global automotive business.

ARM Innovations and the Maker Movement: An interview with Dominic Pajak, Embedded Strategist

I sat down with Dominic Pajak, ARM Embedded Strategist, shortly before Christmas after having watched him "wow" an audience on ARM's support of the Maker Movement. A long-time ARM engineer and the original product manager for the company's Cortex®-M0—he's been in the thick of ARM's success in low-power microcontrollers, sensors and radios. In his new strategist role, he's involved with deployment of ARM's IP into all kinds of cool gadgets and use cases. Oftentimes, he concedes, the journey starts with a Maker who cobbles something together and then drives the prototype to success. Edited excerpts follow.
—Chris "C2" Ciufo, editor

Chris A. Ciufo, Editor-in-Chief, Embedded; Extension Media

Chris Ciufo: Dominic, are you having fun?

Dominic Pajak: I've gone from engineering [ARM] products to working with semiconductor partners…all the way up to talking to people using the end devices. And there are some pretty cool projects being done. So I feel I have been on a journey that is pretty amazing.

I was the product manager for the Cortex-M0. I launched the product and then was very heavily involved in the Cortex-M processor family and later moved into our segment marketing group where we're focused in vertical markets where the devices are deployed. As the journey goes, in the first part of my marketing career I was launching these microcontroller type cores and [saw them] getting a great deal of traction in low power microcontrollers, and sensors and radios. Now I am focusing more on where they are getting deployed, which is really really interesting.

C2: I watched your recent YouTube video and wonder—how do you define a Maker?

Pajak: From my point of view (and I don't speak for everyone who considers themselves a Maker), this is really just a "catch all" label for anyone who has a passion or an interest to understand how things around them work and also to create things. They do this either for fun, or for business, or to solve problems in their homes or their communities. It is a really broad term. And it's not exclusively reserved for a hobbyist. Makers are people who are creating enterprises and products out of [bits and parts] and whatever works.

C2: If that's what a Maker is, how do you characterize the Maker Movement? Is it a fad?

Pajak: The way I would define it is this: "embedded" by its nature is a long tail type market, just like the emerging IoT market. [Editor's note: long tail refers to the shift from a few product or market hits, to a huge number of possibly smaller hits stretching out over time. The long tail successes exceed the shorter hits.] There are some very high volume areas within this, such as wearables, smart cities, or building automation in the home, but there is also a long tail of stuff.

The thing about Makers and part of their philosophy is if you rely on other people to make your stuff, then economics of mass production will shape what you get. They often go for the highest volume product, and that is not always going to cover every person's need. And so the way the Maker Movement would view this is that we now have tools to allow us to prototype and produce stuff in smaller batches to solve problems that are particular to me or to my community.

There are definitely businesses that are possible within this because they are addressing part of this long tail that hasn't previously been addressed. Examples are 3D printing and rapid protoyping tools. Commercial Drone. Or the Pebble Watch. Of course sometimes these products do become high volume.

But the Maker Movement also includes STEM education along with hobbyists that are just interested in doing stuff for the fun of learning and maybe solving things around their own home. They're not necessarily entrepreneurs

but they would still be classified as Makers. The Maker Movement is very broad, but this is how I see it from my vantage point in ARM.

C2: Can you give me an example of a Maker product that was more than a hobbyist's project?

Pajak: We have a Kickstarter page on the ARM Connected Community that was launched last week, and I had an interview with Pebble's CEO and he talks about how in his dorm room he had this idea for a wearable, a connected watch. Then he prototyped it with an Arduino and he raised over $10 million through Kickstarter. This is an example of someone who has taken the accessible technology and platforms to prototype an idea and then has gotten the backing of a lot of people to go and make this thing a reality. It really gives a good picture of how the Maker Movement can be considered the sharp end of where [some] innovations are coming from.

The democratization of technology means these platforms are not just accessible to electronics engineers. People with other disciplines can also get access to them to prototype with, experiment with, and apply technology to new domains. This is where you are seeing crossovers into wearables—like Pebble—into fashion, or into medicine.

One of the notable Kickstarters you will see is a device called the qPCR DNA diagnosis machine. This project is funded to create low-cost DNA diagnosis machines. Some versions of the machine are based on an ARM Cortex-A8 on a BeagleBone Black. This is an accessible platform that people in biomedical sciences have taken to create something which is very disruptive but has really positive transformative potential to do good for society. This isn't just about pure commercial drivers; there is also a huge human factor.

C2: What is it about ARM and your ecosystem that allows somebody who may not be an engineer, but who may even be an artist, actually create something and achieve such success?

Pajak: We are working to abstract the technology and make it easier, through tools such as mbed™IoT Device Platform. There are several really good reasons for our successes and I'd like to explain. One is about choice and simply the diversity of the different parts the ARM partnership brings to bear. With the Internet of Things (IoT), for example, it isn't a one size fits all thing: we're spanning from swallowable medical devices, wearables and implantables, to pet trackers and connected cars, in all sorts of different shapes and sizes.

C2: How has ARM's low-power reputation aided the Maker Movement?

Pajak: If you take a look at the teardown of any of these leading-edge wearable devices, you will see an ARM-based device inside. People developing these products are pushing back the boundaries of where technology is being applied, and if it is a wearable or a remote IoT device it can be battery powered. That's an essential metric when they are creating these devices and [trying to] really squeeze down the form factor to something that fits seamlessly and unobtrusively into people's lives. The battery is really a key concern, and so ARM's energy-efficient background is well positioned to address pushing the boundaries where this technology has been or is going to be applied.

You see this low-power capability at its most powerful with people from cross disciplines, not just EEs, but also now industrial designers, fashion designers, or product designers. People across many disciplines apply this technology to their domains of expertise and to the problems they see. The diversity that ARM has and the fact that we can offer this low-power capability means they can squeeze [it] into smaller form factors and address the problems very efficiently.

C2: What's on your list of the top 5 benefits that ARM brings to the Maker community?

Pajak: We just talked about one: diversity and choice.

We also discussed energy efficiency through ARM's low-power reputation, and this is of huge importance. Crafting your design to the maximum functionality, longest battery life, and at an optimal price point. That comes back to diversity as well because you need the right choice of parts in order to craft your designs. Another one is accessibility. And so, making [all of this] accessible in terms of cost. There are extremely low-cost ARM development boards available today. One of our mbed boards—I believe from Freescale—is $12.00. But it doesn't end there.

The Raspberry Pi, which is based on ARM11™ Broadcom parts, I hear can be purchased for as low as $25.00 for the Model A+. Raspberry Pi is a fantastic vehicle, and has a very respectable mission in education by giving access to computing at a low cost. You have Arduino, which is extremely famous for bridging the world of electronics and design. And you'll have seen this year they launched the Arduino Zero, which is based on ARM Cortex-M0+. They have the Arduino Due, which is an ARM Cortex-M3. And then the Tre, which is going to be ARM Cortex-A8. So ARM offers accessibility to Makers through lots of different easy-to-use vehicles; people can get hold of ARM technology and innovate around it.

C2: You've mentioned three benefits. Is ARM's position in mobile a big factor?

Pajak: Absolutely. Another key benefit to Makers has to be our position in mobile. That's a springboard to so many things we offer to embedded Makers. ARM is the global leader in these low-power connected devices. We have an extremely well established position in mobile and embedded. Last year alone, the ARM partners shipped 10 billion ARM-based chips. Which is a lot of chips. 3 billion were Cortex-M actually, so we shipped more than that into the overall embedded markets because we span from low-powered Cortex-M and up to Cortex-A which is more suitable for these richer interactive kind of media nodes.

So this industry-proven technology invites some reuse, for certain. Chris Anderson, who is a former writer and Editor-in-Chief of Wired and now is the CEO of 3DR, makes a very interesting point about the economies of scale of mobile. The investment that ARM has made with its partners into efficient computing for mobile has a lot of reuse in the Internet of Things types of markets (such as wearables).

C2: So is there a 5th benefit? Would you maybe include your ecosystem of partners?

Pajak: That is where I was going to go. So, obviously software is vital to these systems. It's one thing to stitch the hardware together into your vision, but people still need an ecosystem of tools and OS providers to span all this stuff. Giving people choice in hardware is fantastic, but having software on a standard architecture makes it incredibly powerful.

If you were to look at the plans around mbed that were announced at TechCon, you will see there's already a very strong ecosystem around this—spanning from sensor providers, communications providers giving Bluetooth, Wi-Fi, cellular, all the way right up to account service providers. And so, it's important for this generation of IoT devices where we know that Makers want their end devices to integrate communications and sensors and they expect to compute very quickly. But we also know they want to connect [the bits] seamlessly, securely and efficiently for the Cloud. This is very much the focus of mbed, and you will see we've got some really fantastic announcements and products coming down the line.

By the way, security is front-and-center of the way they're approaching this and actually [the mbed] approach brings the same class of security you would use for your banking on the Internet down to these constrained devices.

C2: Earlier, you said you were excited about ARM and your job. Why?

Pajak: Certainly the most exciting part to me is that while the typical person on the street doesn't know what a microcontroller is, they may now know what Arduino is. And that is incredibly powerful because suddenly no matter what your discipline might be—artist or designer, for example—you can understand the power of the physical computing that might bring to your particular application area. The other exciting thing is helping educate people on the fact that computing is now so low cost, so small, so potentially "embeddable" in all these different products. This is an interesting point in history actually, where the technology is crossing over to all these disciplines. And ARM is right in the thick of it.

C2: Wearables is one of the first to have emerged from that.

There are other examples. Technology is bringing efficiencies to systems that were probably fixed in the past like garbage collection, making maintenance rounds or the trucks that are going around filling oil tanks. One example I heard was in Minnesota, where the oil delivery truck knows the customer's tank status in advance [remotely] so the route can be optimized to make sure the people who need the oil most get their tanks serviced and are kept warm. With this technology-enabled optimization, it also burns less fuel in the delivery fleet. But there are countless examples of this kind of efficiency and how technology is democratizing the status quo.

C2: What are some of the technologies still needed to keep the Movement going?

Pajak: There's a need for open standards for device communication, and interoperability is necessary to allow this trend to scale. Although not a technology per se, I think education is a big one. And the approaches that are going to be required of the future development of the Internet of Things and these kinds of interactive, interconnected devices is very different in some ways from traditional embedded engineering.

Now you need to be paying more attention to how [your design] is interacting with an Internet-connected system. You need to be thinking more about interaction design with the environment and with people, and it's really the human element that is critical here. We have to think about the value it is bringing businesses and the experiences it's bringing to people. I think more of a rounded perspective is needed, not just from the technical perspective.

It's also essential to be aware of what data is being generated and how can it best be formatted, especially targeting big data analytics. Some other questions that we need to educate system designers and Makers on is: How can we optimize a bigger system? How can we integrate with the existing IT systems that enterprises have? There is a need for a much more broader view when you're connecting these products.

C2: Any last thoughts?

Pajak: Two things. One that is fresh in my mind is last week we launched a curated page on Kickstarter.com, and to me this is amazing because there are 50 independent projects that are are basically start-ups, entrepreneurs. Some of them are small- to medium-size enterprises that have cool projects and they have just chosen to use ARM. They've just evaluated the technology, and the optimal solution is available from ARM partners, so they've based their products on it. Some of these products are absolutely amazing. One is FLUX, which is a 3D printer and scanner. So you put an object in there and it will scan it and then it will print it.

The other thing is how traditional product R&D is being supplemented and sometimes supplanted by a Maker approach. Just look at the amount of VC funding going into hardware startups, especially after Kickstarter campaigns. Crowdfunding has revolutionized the way the product design is happening. It can be far more nimble to have your idea and put it out to a consumer base and immediately get feedback, immediately get buy-in for that product to be funded. It strikes me that this methodology is not just for the startups and the hobbyist. This is something that major companies are looking at very seriously as a means to innovate more quickly.

This article was sponsored by ARM.

GainSpan Corporation

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

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

FEATURES & BENEFITS

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

TECHNICAL SPECS

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

APPLICATION AREA

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

AVAILABILITY

Sampling now with production slated later this year

CONTACT INFORMATION

GainSpan Corporation
3590 N. First St., Suite 300
San Jose , CA 95134 USA
1-408-627-6500 Telephone
sales@gainspan.com
www.gainspan.com

We simplify the use of embedded technology

FAST AND COMPACT
conga-TC97

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

HIGH END PERFORMANCE
conga-TS87

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

POWERFUL AND SMALL
conga-MA3/conga-MA3E

- COM Express Mini Type 10 module
- Intel® Atom™ and Intel® Celeron® processors
- Gen 7 Intel® HD graphics
- Extended temperature range option

HIGH PERFORMANCE QSEVEN
conga-QA3

- Qseven module
- Intel® Atom™ and Intel® Celeron® processors
- Gen 7 Intel® HD graphics
- Extended temperature range option

Find more details at: **www.congatec.us**

congatec Inc. | 6262 Ferris Square San Diego | CA 92121 USA |
Phone: 858-457-2600 | sales-us@congatec.com

intel IoT Solutions Alliance

congatec