FREE Download www.iotworld.be

IoT World

Internet of Things from A to Z

Systems - Modules - Gateways - Chips - MEMS - Sensors
Software - WEB Services - Cloud - Service Providers
IoT & M2M Customer Applications - Market Worldwide

IoT World is a Global Publication of e2mos

March 2016

In this issue

Create and connect your Things. Fast!

Enterprise grade IoT solutions for the large community of developers, education facilities and enterprise customers

LoRa Radio - Bluetooth and WiFi CortexM4 based

Highly scalable multi-network solutions

Ideal for urban or remote areas/coast lines and where traditional cellular connectivity alone is unable to resolve

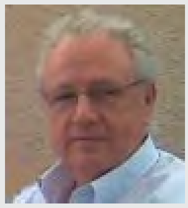
Internal and External Antennas

Exclusive interview with Fred de Haro, CEO of Pycom
see page 10

pycom™

The Internet of Things will connect Billions of Devices,
IoT World is connecting you with your Next Customers & Partners TODAY

... in this issue:



Daniel Dierickx
CEO & co-Founder
at e2mos
Acting Chief Editor

Dear Reader,

Here is your free copy of IoT World, one of our four magazines published by e2mos.

Our aim is to provide you with relevant information in relation with your activity.

Those magazines are part of the e2mos « Go-to-Market Platform »

This GLOBAL Platform is a UNIQUE Set of Services for ICT, Embdded and IoT Vendors from Multicore to Application-ready Systems & Servers.

Our WORLDWIDE Services include:

- Business Discovery with Customer Meeting Setup
- Telemarketing
- Call Campaigns
- Massive e-mailings Worldwide
- and our four magazines, each magazines has its own Website (see page 11)

It is all based on:

- 30+ Years Customer Relationship and Market & Technology Expertise
- our PREMIER Database started in 1980 and maintained EVERY DAY with many sources « Anything less will not do »

More www.e2mos.com

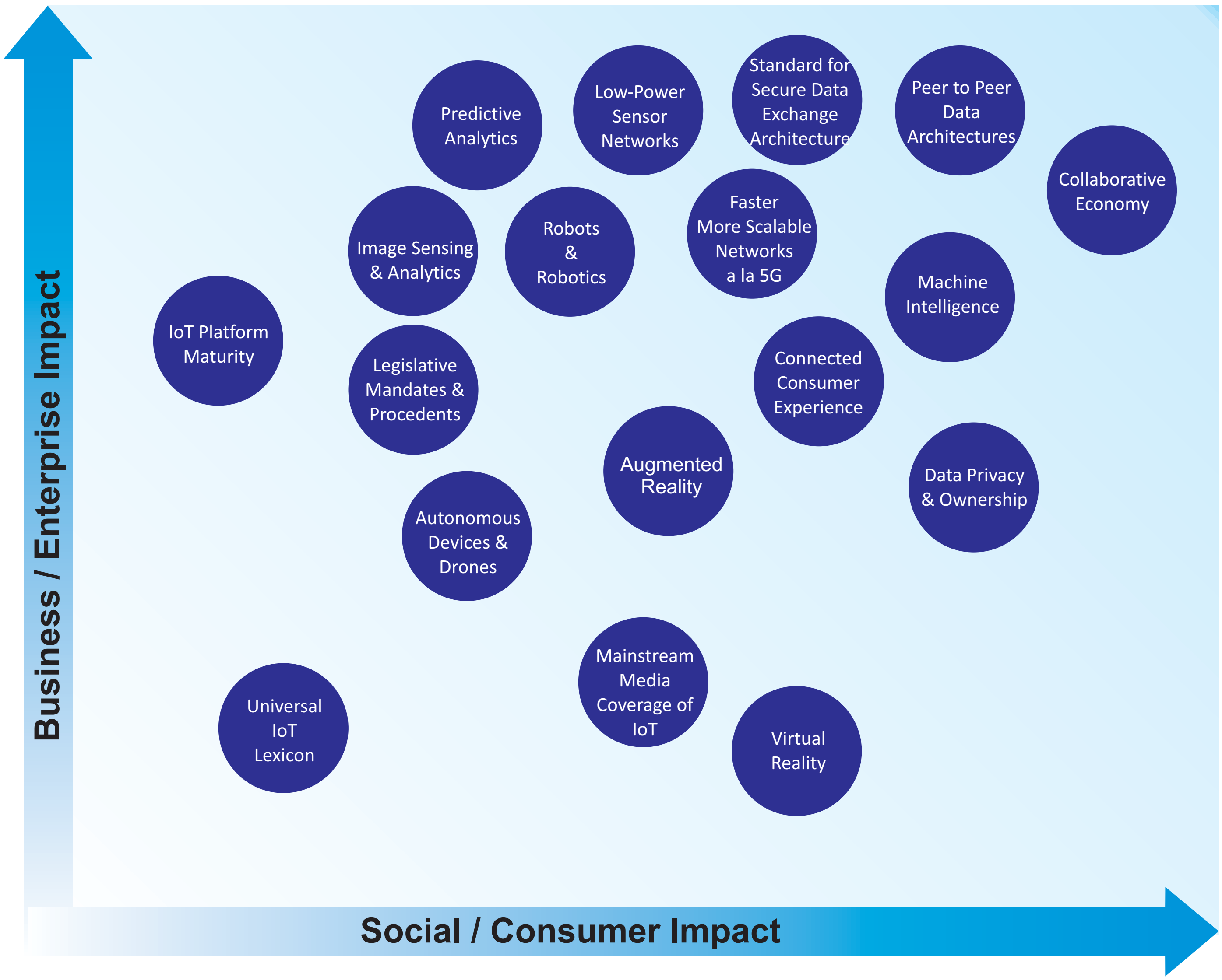
Thank you.

Editor/Publisher: e2mos
www.e2mos.com
Contact: mgt@e2mos.com

Harbor Research's Internet of Things Trends Report
The Top 18 Trends to Watch in 2016

By Jessica Groopman & Glen Allmendinger - January 2016
Here is an introduction, the full report can be downloaded see page 4

Trends Impacting the Future of the IoT - Enterprise versus Consumer



This image depicts a variety of themes addressed in this report. The vertical axis represents the impact such trends will have on enterprises and business, while the horizontal axis represents the consumer and social impacts such developments will have. Harbor Research predicts the likelihood for widespread adoption of these trends depends directly on the impact they will have on both businesses and consumers.

From our perspective, 2016 is ripe for continued evolution—not just around the application of sensors on 'things,' but around the myriad of forces and entities inherent in the entire ecosystem driving a more connected world. From technological advances, to market proliferations and consolidations, to societal constraints to economic pressures, the analysts at Harbor Research have compiled the top 18 trends and movements in 2015 that will define the Internet of Things in 2016 and beyond.

1. **IoT tiptoed into the mainstream in 2015.** From SuperBowl commercials to political debates to Fitbit's IPO to the Connected Home section at BestBuy, the Internet of Things reached into mainstream culture in 2015.
2. **2015 brought the greatest adoption of connected products and services to date.** Thanks to sharp declines in the cost of sensing technology and data processing, Harbor Research finds some 3B connected devices came online in 2015, with significant adoption across both Transportation and Buildings sectors.
3. **Confusion around what IoT is (or isn't) persists.** Despite massive investment and adoption, most people are still perplexed by what the Internet of Things (or should we call it Digital Transformation? Industry 4.0? Machine to Machine?) actually means.

... to Page 4

... from Page 3

4. **The Internet of Things dominated mergers & acquisitions in 2015.** The M&A climate of 2015—one of numerous divestures and megamergers, particularly in the semiconductor space— can well be characterized by movement directly related to the Internet of Things.
5. **2015 brought legislative rumbles to the IoT space.** World over, governments are struggling to address the Internet of Things. Yet, 2015 brought significant legislative movements primarily in the areas of data access and security.
6. **The IoT platform space exploded in 2015, but it's still highly fragmented.** Proprietary development and acquisition by tech giants call attention to the IoT platform space; meanwhile, hundreds and hundreds of new IoT platform innovators continue to proliferate.
7. **Consumer IoT and Industrial IoT are colliding.** From Apple Watch for field technicians to Microsoft Kinect in the grocery store, enterprises are applying (and saving costs) with consumer technology. Although consumer and industrial IoT have been largely bifurcated in ecosystem, adoption, and investment, 2015 saw the beginnings of the end of this distinction.
8. **Blockchain sets the precedent for a digital economy (way beyond Bitcoin).** The information architecture inherent to Bitcoin provides a powerful precedent for the development, contextualization, exchange, and security of data needed for IoT.
9. **The Collaborative Economy booms... and provides a precedent for IoT.** Despite regulatory constraints, 2015 saw continued disruptive growth of 'shared' services, illustrating the power of collaboration and ecosystems, made possible by precisely the same components inherent to IoT architecture.
10. **Customer experience is evolving in the direction of IoT.** From retailers incorporating sensors into mobile appls to chip cards and mobile payment redefining the transaction process, 2015 brought a number of important developments in the evolution of 'customer experience,' many driven by IoT technologies.
11. **5G, the next cellular generation is taking shape.** Mobile operators are vying to achieve super fast, efficient, and flexible data networks in order to adequately support IoT applications at scale. Meanwhile, alternative connectivity protocols are evolving rapidly.
12. **Machine Intelligence evolves into 'killer' software app:** Computers are learning to read, write, learn, think, and even understand human sensor input such as touch or hearing. Today companies are buying 50x more data to train AI programs in development than they were just 3 years ago.
13. **Image will be the next frontier of data capture, but remains infantile.** Many of the emerging technologies of the past few years— 3-D technology, cameras, facial recognition, computer vision, augmented reality, image & video analytics—are all components to sensing and analyzing the look and feel, (not just the sentience or behavior) of our digital and physical worlds. Still, immediate technological, economic, and societal hurdles remain.
14. **Robots are emerging (beyond manufacturing).** 2015 saw emergence of robots in new industries such as retail, hospitality, and healthcare, bringing us telebots replacing call-center agents, connected industrial floor cleaners, automated guided vehicles (AGVs), robotic retail associates, and a host of robotic "personal assistants."
15. **Augmented reality poised to accelerate in 2016.** 2015 brought significant movement for the AR space with numerous brand experimentations as well as major acquisitions and movement on the part of Google, Apple, and PTC. Already, a variety of other technology companies have announced they'll be following suit in 2016.
16. **Drones (and drone investment) took off in 2015.** From legislative movement to retailer experimentation to consumer adoption, the year brought shocking growth to a technology segment which, just a few years ago, was expected to putter along. Investment grew nearly tenfold in 2015 alone.
17. **'Low Power:' A most powerful (but challenging) catalyst.** 2015 brought the rise of Sigfox, greater adoption of low power beacons, and significant attention to edge computing, but the fate of IoT still remains at the mercy of more efficient distributed power consumption at every level: connectivity, hardware, chip, battery, storage, etc.
18. **IoT is pushing movement across the value chain.** 2015 brought numerous examples of traditional companies driving bottom line growth (to core products and services) by investing, integrating, acquiring, or expanding into entirely new offerings and relationships.

Trends and forces shaping IoT in 2016 abound. The deeper business and societal opportunities of data generated by connected interfaces and devices far transcend the endpoints (e.g. products) themselves. The real value potential in an IoT-enabled world lies in the services made possible—via collaboration, partnerships, predictive intelligence, and entirely new value-adds, offerings, and business models. Ultimately, the 'many-to-many' model of the Internet of Things requires a narrative shift. It requires a disruption to the current way of doing things; our existing paradigms around who should pay, 'core competency,' security, privacy, [data] ownership, technological architecture, and many other market levers. These themes pervade the trends discussed above, and will continue to define IoT adoption in 2016 and beyond.

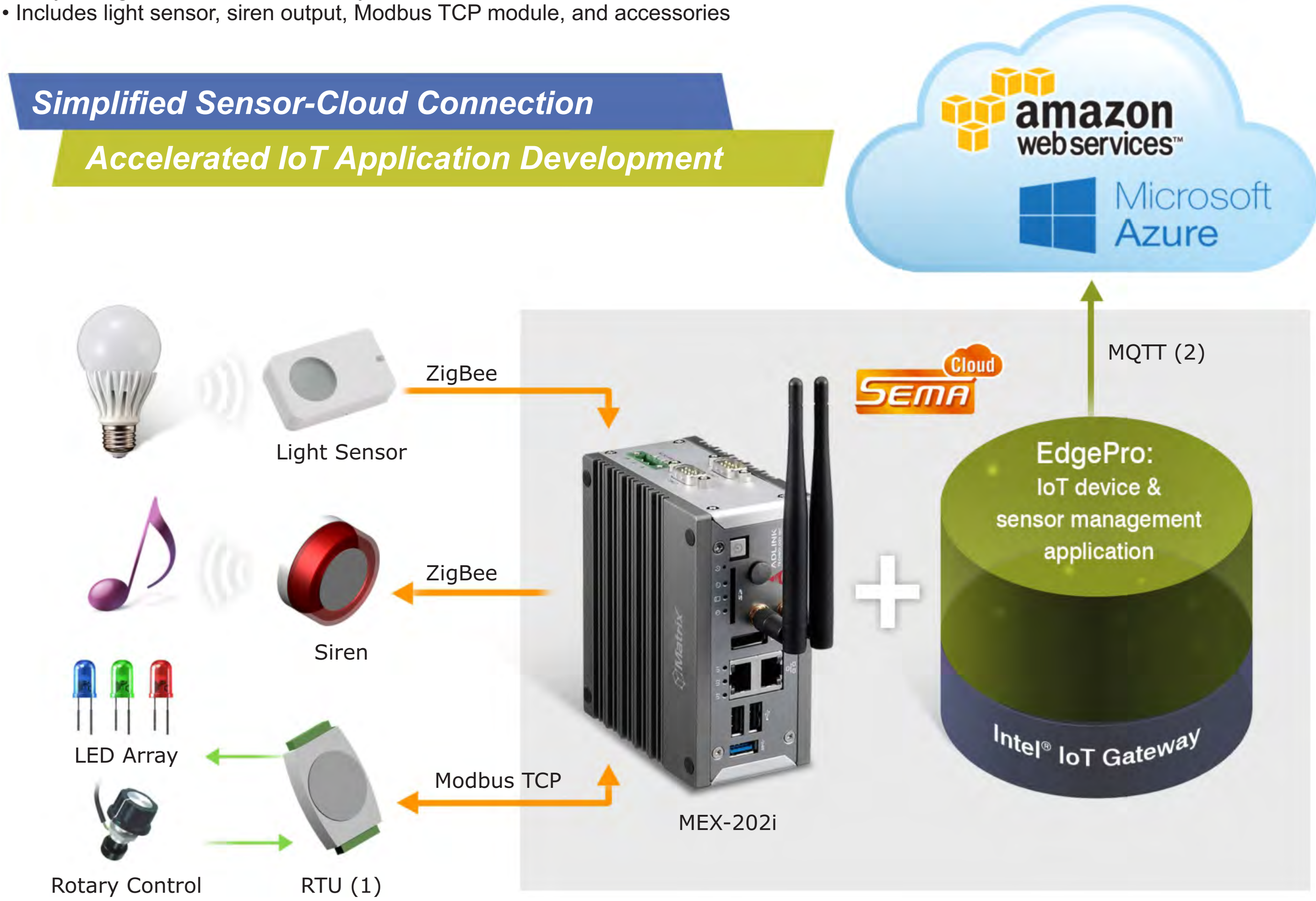
Access Harbor Research's full 2015-2016 trend report, including examples & analysis of each trend HERE

Intelligent IoT Gateway Starter Kit
End-to-End Solution from ADLINK

The Starter Kit contains Intelligent IoT Gateway MXE-202i, EdgePro IoT Device and Sensor Management Application based on Intel® IoT Gateway

Features:

- Provides a complete IoT connection solution for accelerated IoT application development
- Equipped with MXE-202i (Box Computer)dual-core Intel® Atom™ SoC processor E3826 IoT Gateway on Wind River® IDP XT 2.0
- Preloaded ADLINK EdgePro IoT device & sensor management application
- Easy configuration with user-friendly administrator interface and dashboards
- Includes light sensor, siren output, Modbus TCP module, and accessories



(1) RTU: Remote Terminal Unit
(2) MQTT is a machine-to-machine (M2M) "Internet of Things" connectivity protocol

The Intelligent IoT Gateway Starter Kit includes:

- MXE-202i with dual-core Intel® Atom™ SoC processor E3826 IoT Gateway on Wind River® IDP XT 2.0 + 8G SD card
- Preloaded ADLINK EdgePro IoT device & sensor management application
- WiFi/BT Kit (pre-installed)
- ZigBee / 802.15.4 Module USB Adapter
- Modbus RTU module
- ZigBee wireless light sensor
- ZigBee wireless siren
- Rotary control
- LED array
- Ethernet cable
- 40W AC/DC adapter

More:

- Press Release Click Here
- Technical overview Click Here
- Datasheet Click Here

Contact

ADLINK Technology, Inc. - Taiwan
Tel +886-2-8226-5877
Fax +886-2-8226-5717
Email service@adlinktech.com

Ampro ADLINK Technology, Inc. – USA
Tel +1-408-360-0200
Toll Free +1-800-966-5200
Fax +1-408-360-0222
Email info@adlinktech.com

LiPPERT ADLINK Technology GmbH - Europe
Tel +49 621 43214-0
Fax +49 621 43214-30
Email emea@adlinktech.com

INTERNET OF THINGS (IoT) DESIGN CONSIDERATIONS FOR EMBEDDED CONNECTED DEVICES

ANDREW CAPLES SENIOR PRODUCT MARKETING MANAGER, NUCLEUS @ MENTOR GRAPHICS

INTRODUCTION

While we hear many promises of what the Internet of Things (IoT) will bring, the potential behind the IoT is hindered by the complexity of machine-to-machine (M2M) device software. Many early M2M systems consisted of remote devices in segmented networks relaying information back to a computer for supervisory decisions. For these systems, decisions were centralized, information flowed primarily one-way, and network segmentation provided adequate security. M2M did not rely on the public Internet so a "private" network with the proper precautions was all that was needed.

The emergence of the IoT today has changed the traditional M2M paradigm. The sheer breadth of M2M features now requires software developers to integrate code from numerous sources including home-grown, commercial, and open source in order to build devices that are connected, secure, and capable of making decisions. Unlike traditional M2M systems, the IoT model includes bidirectional data flow and relies on public networks to transmit much of the data. The promise of the IoT will allow smart grids to interact with home area networks in an effort to minimize energy consumption, vehicles will communicate with other vehicles to circumvent accidents, and remote patient monitors will deliver real time data for cost-effective medical care, to name a few examples.

The software required to build these connected IoT devices – devices that are secure and capable of autonomous network insertion in order to exchange information and services – is in great demand today. The promise of the IoT won't be fulfilled until integrated software platforms are available that allow software developers to develop these devices efficiently and in the most cost-effective manner possible. And at the same time, meet the growing list of expanding M2M and networking requirements.

M2M FEATURES - FAR MORE COMPLEX IN AN IoT WORLD

On the surface the complexity of software can appear daunting. In order for the IoT to live up to its potential, low cost M2M devices will be required to seamlessly integrate onto "server-less" networks and communicate with other networked devices without manual intervention. A few additional requirements include:

- Routine configuration actions, such as IP address resolution, will need to be coordinated by both the existing device on the network and new devices that are introduced without the benefit of a network server managing the activity.
- Once networked, devices will be required to dynamically discover other networked devices and their resources while also introducing their own services. Some IoT protocols will allow devices to act as both a client and server depending on the use case or application.

Security requirements for M2M devices vary based on industry and market segments. However, to maintain data integrity, a few general principles apply:

- There has to be authentication before data transactions and data encryption before transmission to manage passive threats.
- Devices will have to withstand active threats, such as IP storms or floods.
- Because many devices are battery-operated and deployed remotely, power efficient systems must be able to take full advantage of the low power features of the processor and other hardware components in the system.

CONNECTIVITY FOR IoT NETWORKS

IoT networks must be scalable in order to support the dynamic nature of the IoT (as devices are added and removed from the network). For many applications, resource discovery and service announcements will need to be completed autonomously. Fortunately, zero configuration networking protocols such as multicast Domain Name System (mDNS) and DNS-based Service Directory (DNS-SD) support these services and can be used to integrate new devices to an IoT network. mDNS provides a channel for devices to broadcast services data without a centralized server. DNS-SD extends mDNS by providing service discovery. Devices can broadcast their services while discovering the services and resources of other devices.

To facilitate efficient M2M communication, Representational State Transfer (REST) architectures will also need to be leveraged. The benefits of REST include gains in network scalability, performance, and security. Because the REST architecture features a layered infrastructure designed to maintain separation between the client and server, REST-based systems are easily more scalable and support the seamless addition and removal of IoT devices.

It's also worth noting that as devices and various intermediaries are added to the network, the data paths can be altered which may negatively impact system performance. To correct this, caching data on devices closer to the client, such as proxy servers or gateways, network performance will be enhanced, or least maintained as the data paths change. Additionally, through the use of Uniform Resource Identifiers (URIs), network resources can be addressed by IoT clients. Using HTTP for the transmission, resources can be accessed and/or modified through commonly used protocols such as JSON and XML. For added protection, encryption can be used for safe data transmission HTTP(s).

... to Page 7

... from Page 6

IoT SECURITY

Because many IoT devices can be connected on dispersed public networks and support bidirectional data flow, these devices will be highly susceptible to attack. Just look at the network connectivity options today that did not exist 20 years ago; Wi-Fi, ZigBee, Bluetooth, and 4G cellular to name a few (one can appreciate the breadth of devices that will be connected.) Each connectivity option has very clear advantages – as well as disadvantages when it comes to secure communications. Without designing in security methods to address the full of range of threats, IoT devices are vulnerable to attacks from even the most unsophisticated methods. Without question, active and passive threats have to be detected, neutralized, and corrected before any harm to the individual device or the IoT system occurs.

It is essential that checkpoints basic and enhanced security be followed. A few of these checkpoints might include:
• Integration of security protocols for encryption and authentication must always be required.
• Before any data is transferred, the source of the data needs to be verified. The use of public keys and x.509 certificates are an extremely useful tool to verify the source of the data before any exchange is attempted.
• Online Certificate Status Protocol (OCSP) will streamline the client side resources required for x.509 certificate verification, which is significant for IoT devices with limited memory. Because OCSP responses to "authentication requests" it contains less information than a typical Certificate Revocation List (CRL). The complexity on the client side can be reduced by eliminating the need to parse through long lists.
• To address the potential for eavesdropping or other passive threats during a communication session, Transport Layer Security (TLS v1.2) (or OpenSSL) provide the foundation for security by encrypting data before transport. TLS relies on the use of contemporary encryption methods such as Advanced Encryption Standard (AES -256) and 3DES to provide a high level of encryption for IoT devices.

The use of encryption prevents the loss of data to passive listeners, but is does not prevent the alteration of data while traversing the network. Hash functions to generate Message Authentication Codes (MAC) are needed to ensure the integrity of the message and guarantee the content is not altered during transmission. Many networked devices are easily taken down by IP floods, storms, or a barrage of fragmented packets. To address these active threats, IoT devices must be designed to successfully detect attacks to prevent memory overflows or other faults that can disable a system. One way to maintain system integrity against these active threats is to design the device to be certifiable by WurldTech, an authority in IP security.

POWER MANAGEMENT FOR IoT DEVICES

Many IoT systems will be comprised of remote devices on dispersed networks that will act either as sensors, aggregators, and/or gateways. Requirements for these remote devices can include being as power efficient as possible either to extend battery life or to meet green energy goals.

The good news is silicon providers have designed processors with many low-power features including; Clock and Power Gating, CPU idle, Sleep modes, Dynamic Voltage and Frequency Scaling (DVFS), Standby and Hibernate. However, the task to develop a power efficient system falls on the application developer to write code that actually uses the low-power features of the silicon. Typically, application developers receive the system after peripheral drivers, board support packages, or embedded OSes with middleware have already been developed. Unless the underlying software has been designed to take advantage of the low-power features of the silicon, writing power-efficient code at the application level becomes very challenging or even an impractical exercise.

For example, an Operating Point transition (lowering the clock frequency to save power) requires the software to:
• Verify the status of each device on the system to ensure a transition can occur.
• Verify the lowest operating frequency the device can run at based on the current use-case to ensure each device can function at the new frequency.
• Verify the amount of time the device can be taken off-line (park latency) while the system clock is reduced to ensure there is no degradation to system or loss of data.
• Determine the order the device will be taken off-line and brought back on-line based on park latency.
• Recalculate operating parameters, for instance, the baud rate, if the reference was the system clock.

In order to maximize power efficiency, the embedded operating system must include a framework that supports the low-power features of the silicon and provides intuitive APIs. In this way the software developer can create systems that meet the much desired power requirements.

THE NEED FOR A FULL-FEATURED UNDERLYING RTOS FRAMEWORK

The Nucleus® RTOS provided by Mentor Graphics is a good example (Figure 1) of in integrated IoT solution which addresses the various challenges outlined above for developing connected IoT devices.

Nucleus is a widely deployed and scalable 3KB microkernel based RTOS that is designed to meet the M2M device requirements for IoT systems. It has hard, real-time performance and integrated power management services, connectivity support, and a vast array of networking protocols and security.

... to Page 8

... from Page 7

Further, Nucleus fits nicely into a memory constrained MCU-based device, and yet provides the functionality required for IoT systems. A few highlights of this particular RTOS include:

POWER MANAGEMENT The extensive Power Management Framework available in Nucleus (Figure 2) directly maps to the low-power features found in today's more popular hardware. These features include: DVFS, idle, and sleep modes. IoT devices can be placed in various low-power modes through intuitive Nucleus API calls. For complex device transitions, such as moving into hibernate or standby mode, Nucleus provides the framework to safely turn off peripherals, move code into non-volatile memory, and change the operating point of the device.

CONNECTIVITY Nucleus provides support for a vast array of connectivity options including: Wi-Fi, Bluetooth, Bluetooth low energy (BLE), USB 2.0/3.0 for IPv4/IPv6 based networks. Its modular and highly structured organization provides for the ability to install additional software protocols as requirements change.

SECURITY Nucleus delivers end-to-end security options to protect data while in storage or during transmission. Device storage options include password protected secure databases that can store encrypted data. Transmission security includes TLS/SSL with encryption options including, AES-256, 3DES, DES, RC4 and many others. Online Certificate Support Protocol (OCSP) authentication support and Hash functions are available to ensure the integrity of the message and guarantee the content was not altered during transmission.

NETWORKING Nucleus is available with a full featured IPv4/IPv6 stack with over 50 protocols & support for zero-configuration networking that includes mDNS & DNS-SD.

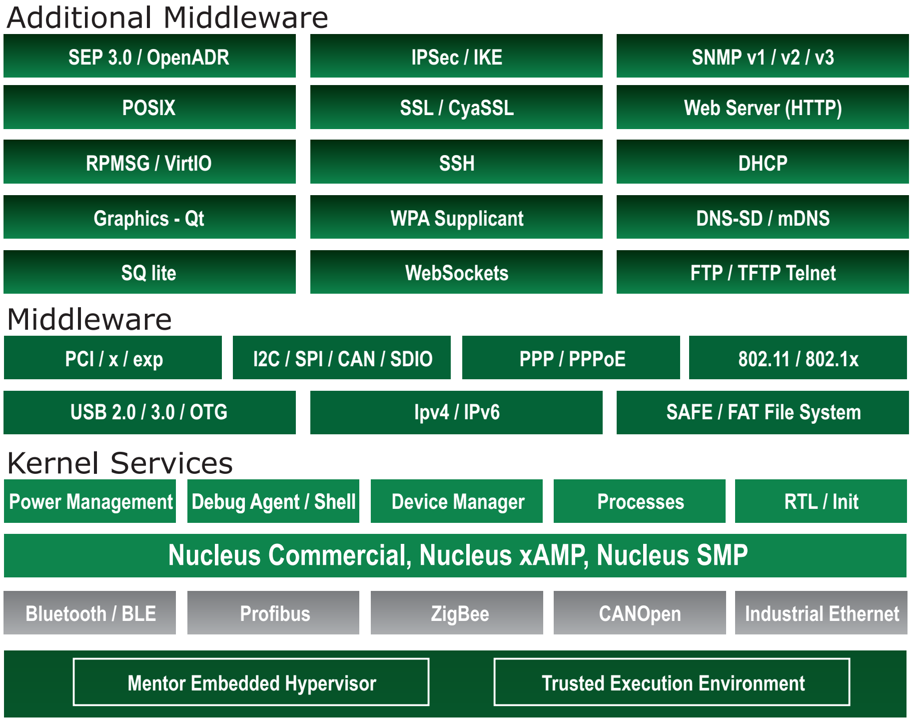


Figure 1: The Nuclues RTOS ecosystem for the development of connected IoT devices.

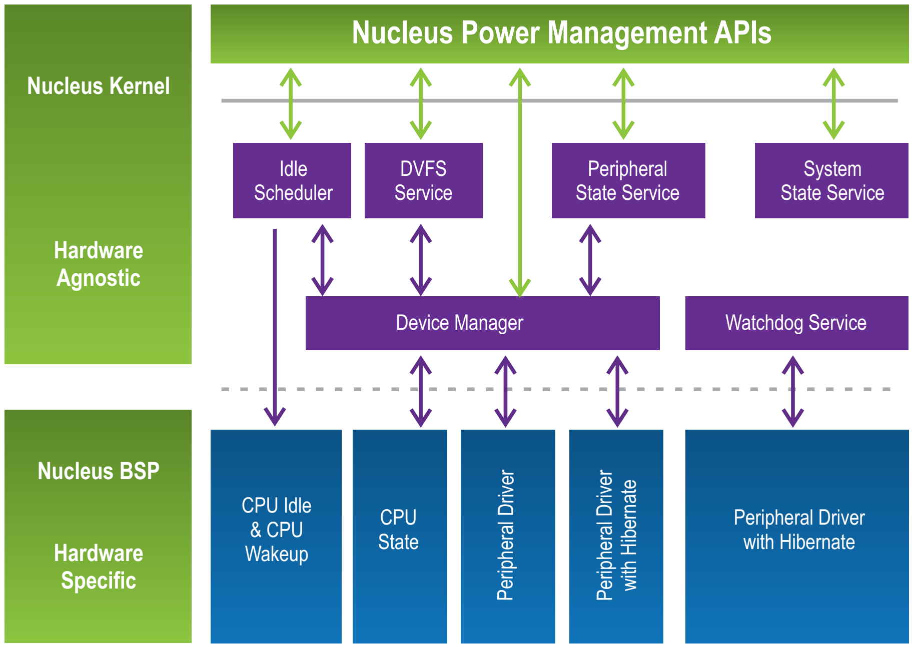


Figure 2: Nucleus Power Management APIs simplify use of power-saving capabilities

CONCLUSION

Software complexity is serving as a headwind for the development of systems that meet the full promise of IoT. Developing homegrown solutions and integrating with commercial and open source code presents numerous challenges and increases developmental risk.

As the market begins to accelerate, the need for cost-effective IoT devices will only increase. The use of a scalable and power-efficient RTOS with extensive networking and M2M protocols is required to develop cost-effective systems that meet the IoT requirements. Gone are the days of a limited or rudimentary OS that once operated a majority of M2M devices. With a full-featured underlying RTOS framework, software developers and design architects will significantly reduce their time to market and still realize all of their IoT application goals.

You can learn more about Nucleus Real-Time Operating System by visiting:
http://www.mentor.com/embedded-software/nucleus

Do you want to connect your career to the Internet of Things?

Are you a digital professional eager to stay up-to-date with the latest trends, tools and techniques in the field of IoT?

The EIT digital professional school offers you a brand-new course "System Architecture for the Internet of Things".

Adapted to the needs of work-life balance, this course allows you to

- Design secure, modifiable, scalable IoT systems that are able to interoperate while meeting quality requirements.
- Apply the best and most modern software architecture methods to design complex IoT applications and 'systems of systems'.
- Understand the business impact of technical decisions made in terms of system architecture.

Unique blended learning at your pace

Developed by leading experts in the field, this course is **tailor-made** and **adjustable to your needs**, schedules and learning pace. Its unique blended learning approach combines online interactive videos, access to case studies, weekly exercises and individual coaching with industry experts, all of which is optional and available for you to access at any time.

Also, you can bring your own project – no matter what stage!

Eager to jump in? Get all the details HERE

The Future of Internet is coming. Are you ready for it?

SIGFOX Adding Germany to Internet of Things Network, Connecting World's 4th-largest Economy and Central Europe

SIGFOX
One network A billion dreams

Labège, France – Feb. 18, 2016 – SIGFOX, the world's leading provider of communications service dedicated to the Internet of Things (IoT), today announced plans to deploy the SIGFOX network across Germany, the world's fourth-largest economy.

The deployment marks the 14th country where the SIGFOX network is deployed or under national deployment. Ambitions are to have the network operating nationwide before the end of 2017.

In addition to bringing the benefits of energy efficient and low-cost IoT wide area network coverage to German companies, entrepreneurs and developers, the deployment will extend the SIGFOX network to a contiguous area of Western Europe stretching from the Mediterranean Sea to Scandinavia.

Full press release click HERE

IoT platform enabling the rapid prototyping and deployment of multi network MicroPython (open source) powered devices

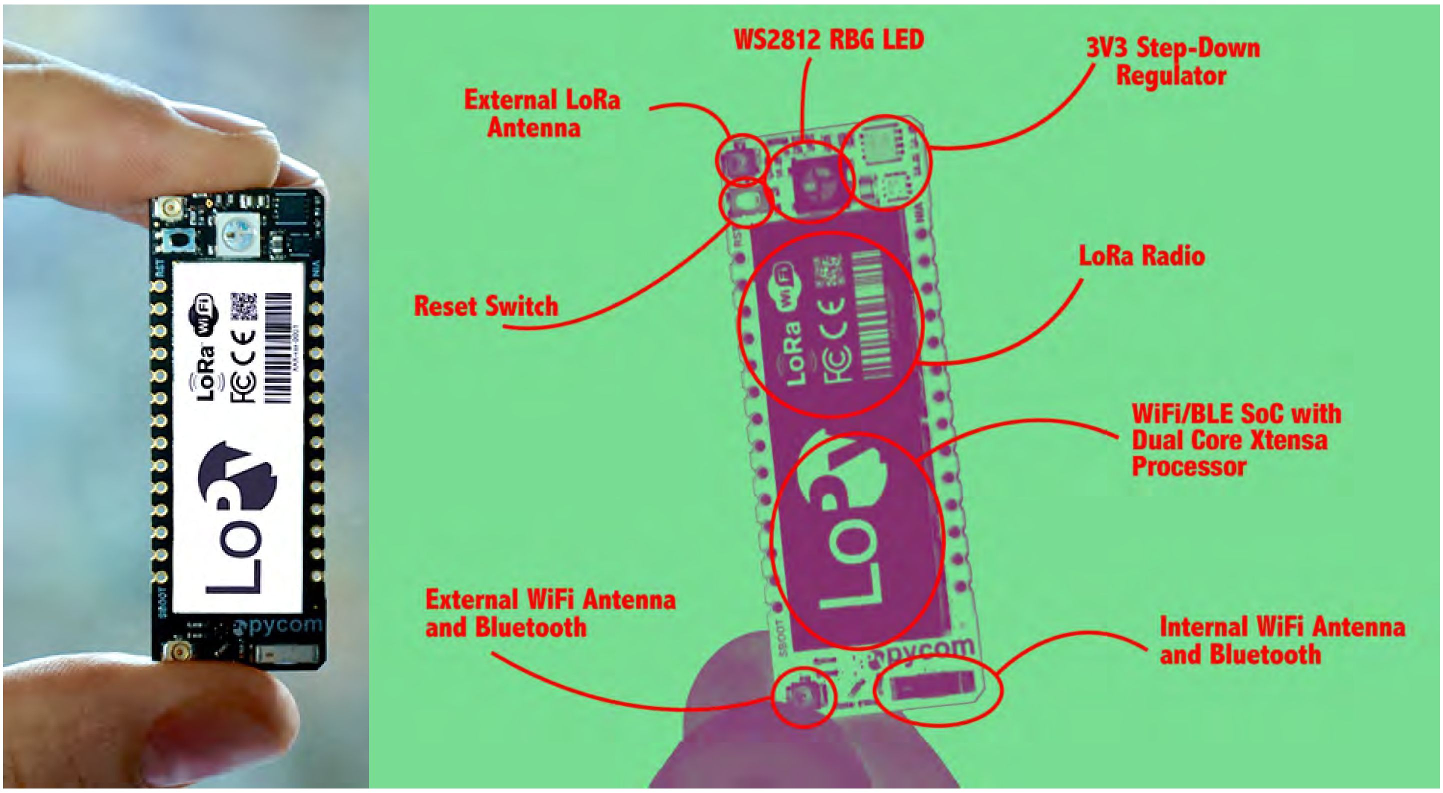
Exclusive interview with Fred de Haro, CEO of Pycom - March 2016

Pycom delivers an IoT platform enabling the rapid prototyping and deployment of multi network MicroPython (open source) powered devices. These are supported by an IDE (Pymakr), a comprehensive library of industry specific applications to further support the large community of developers, education facilities and enterprise customers all of whom are looking to deploy enterprise grade IoT solutions.

Set up in late 2015 and based in both the Netherlands and the UK, Pycom was created by a team of passionate individuals with backgrounds ranging from engineering, technical design, sales and marketing. To date the company has successfully launched two Internet of Things (IoT) products on Kickstarter, the WiPy (WiFi based) and the LoPy (LoRa/Bluetooth and WiFi).

The company has already secured an installed base of several thousand developers and SME customers spread across 56 countries as a result of the innovative IoT development modules it has launched. Pycom joined the LoRa alliance earlier this year and is now in discussions with three LoRa network operators regarding the certification of its products onto those networks, both in the US and Europe.

Pycom delivers its products and services to three key target markets: Developers, Enterprises and Education. Whilst other companies may also claim the same market focus, few are able to offer the scalability in both product and technology, which give a hobbyist developer the ability to bring out an enterprise grade connected device overnight.



This is due to the rapid development cycles achieved using MicroPython, which have seen traditional development timelines shortened by a factor of 10 - a case proven when the company recently delivered a fully working connected product to a customer within three weeks, something which would have historically taken seven months. Furthermore, the unique nature of the multi-network connected boards, which the company specialises in, allows customers to deploy these assets into the market knowing that through the use of one of the wireless networks provided, they can be sure to retrieve/manage their Things' data.

The company is actively working with Enterprise companies looking to resolve connectivity issues experienced as a result of IoT deployments within Urban or remote areas/coast lines and where traditional cellular connectivity alone is unable to resolve.

... to page 11

IoT platform enabling the rapid prototyping and deployment of multi network MicroPython (open source) powered devices

Exclusive interview with Fred de Haro, CEO of Pycom - March 2016

... from page 10

Large isolated landscapes of terrains means traditional cellular (alone) struggle to provide reliable connectivity due to patchy coverage, whereas urban based applications struggle due to challenges such as saturated cellular masts, dense building and assets located underground. Therefore Pycom is working across agriculture, healthcare, retail and smart city segments to ensure companies have access to low cost and highly scalable multi-network solutions.

Many companies claim to be targeting developers and enterprises, so what makes Pycom unique? Well for starters, it has a growing community of developers using Pycom products launched on Kickstarter, the most recent one, the LoPy, being fully funded in just five days.

“It's very encouraging to gather so much support for our vision of connecting developers and enterprises” says Fred de Haro, CEO of Pycom. “We've had so many great comments along the way, but one that stands out for me was one where a backer said he was so pleased he had finally met a company that “understands makers” – what an endorsement. Giving companies and developers multi-network connectivity does not need to come at a price premium if the product is intelligently designed and manufactured from the onset. Suppliers of IoT solutions must start thinking out of the box. Whilst much of the industry's institutional investment has been focused on middleware platforms (all 550 of them), it's vital we start addressing the major flaws on today's hardware platforms - that's what Pycom is doing”.

The company released in 2015 a WiFi based IoT development module using the Texas Instrument CC3200 Coretex-M4 chip. In February 2016, they launched LoPy, the world's first triple bearer (Lora, WiFi and Bluetooth) Micropython nano gateway, which allows users not only the ability to connect their devices to Low Power WAN networks at a range of 40KM, but also to operate and put in place their own LoRa networks within a 5KM radius connecting back to the internet via WiFi/DSL. Pycom recently revealed that the SoC chosen for the LoPy, was the highly acclaimed Espressif ESP32, a chip likely to power other Pycom devices.

Finally, the company has confirmed that later in 2016, they will release their first cellular dev board however expect a twist on that, something along the lines of a good Hitchcock film, as one thing is certain, it will not be a cellular board alone!

More about Pycom and prodts: http://www.pycom.io/

Interview and reporting
Daniel Dierickx

pycom™
LoRa Alliance

About us

Editor/Publisher: e2mos
www.e2mos.com
Contact: mgt@e2mos.com
4 FREE e-magazines
Click on the Logo 's

IoT World
Telecom COTS World
Broadband Broadcast IoT Convergence
Embedded Systems World
ATCA World

LoRa® Technology

LoRaWAN™ is a Low Power Wide Area Network (LPWAN) specification intended for wireless battery operated Things in regional, national or global network. LoRaWAN target key requirements of internet of things such as secure bi-directional communication, mobility and localization services. This standard will provide seamless interoperability among smart Things without the need of complex local installations and gives back the freedom to the user, developer, businesses enabling the roll out of Internet of Things.

LoRaWAN network architecture is typically laid out in a star-of-stars topology in which gateways is a transparent bridge relaying messages between end-devices and a central network server in the backend. Gateways are connected to the network server via standard IP connections while end-devices use single-hop wireless communication to one or many gateways. All end-point communication is generally bi-directional, but also supports operation such as multicast enabling software upgrade over the air or other mass distribution messages to reduce the on air communication time.

Communication between end-devices and gateways is spread out on different frequency channels and data rates. The selection of the data rate is a trade-off between communication range and message duration. Due to the spread spectrum technology, communications with different data rates do not interfere with each other and create a set of "virtual" channels increasing the capacity of the gateway. LoRaWAN data rates range from 0.3 kbps to 50 kbps. To maximize both battery life of the end-devices and overall network capacity, the LoRaWAN network server is managing the data rate and RF output for each end-device individually by means of an adaptive data rate (ADR) scheme. National wide networks targeting internet of things such as critical infrastructure, confidential personal data or critical functions for the society has a special need for secure communication.

This has been solved by several layer of encryption:
• Unique Network key (EUI64) and ensure security on network level
• Unique Application key (EUI64) ensure end to end security on application level
• Device specific key (EUI128)

LoRaWAN has several different classes of end-point devices to address the different needs reflected in the wide range of applications:
• Bi-directional end-devices (Class A): End-devices of Class A allow for bi-directional communications whereby each end-device's uplink transmission is followed by two short downlink receive windows. The transmission slot scheduled by the end-device is based on its own communication needs with a small variation based on a random time basis (ALOHA-type of protocol). This Class A operation is the lowest power end-device system for applications that only require downlink communication from the server shortly after the end-device has sent an uplink transmission. Downlink communications from the server at any other time will have to wait until the next scheduled uplink.
• Bi-directional end-devices with scheduled receive slots (Class B): In addition to the Class A random receive windows, Class B devices open extra receive windows at scheduled times. In order for the End-device to open its receive window at the scheduled time it receives a time synchronized Beacon from the gateway. This allows the server to know when the end-device is listening.
• Bi-directional end-devices with maximal receive slots (Class C): End-devices of Class C have nearly continuously open receive windows, only closed when transmitting. Class C