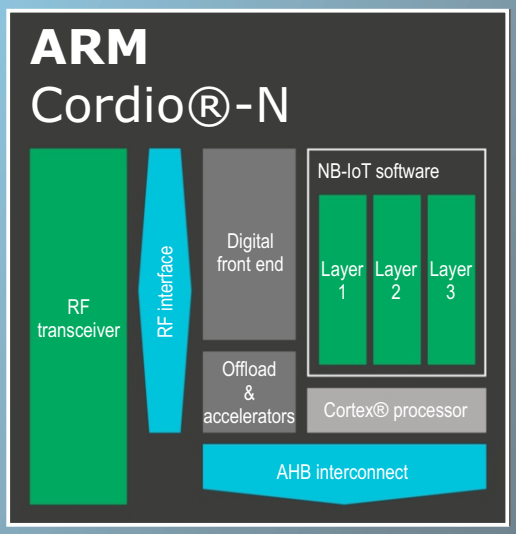
FREE Download www.iotworld.be

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

May-Jun 2017

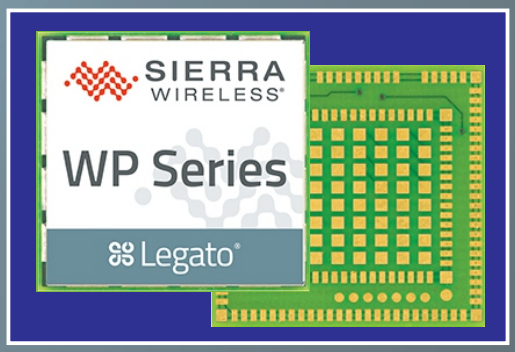


■ Enabling mass IoT connectivity as ARM partners ship 100 billion chips.

■ How to update a billion devices in field.

■ ARM acquires Swedish Mistbase and English NextG-Com to bring NB-IoT compliant technology to ARM-based chips.

■ Introducing Google Cloud IoT Core: for securely connecting and managing IoT devices at scale.



■ Sierra Wireless announces industry's first global dual-mode LPWA module with integrated application processing and GNSS. Supports booth LTE-M and NB-IoT.

Top Linux IoT Projects

■ It's a Linux world, and the rest of computing is just living in it. The Linux Foundation lists 7 top projects as key players in the march of connected open-source systems.

In this Edition:

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

Dear Reader,

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

Our aim is to provide you with relevant information directly 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 Telecom ICT, Video Broadcast, Embedded Computing, IoT and AI Vendors from Multicore Chips to Application-ready Systems & Rack Space Servers.

Our WORLDWIDE Services include:
• Business Discovery
• Customer Meeting Setup
• Telemarketing
• Call Campaigns
• e-mailings Worldwide
• and our 5 e-magazines, each magazines has its own Website (see below).

It is all based on:
• 30+ Years Customer Relationship and Market & Technology Expertise
• our PREMIER Database started in 1980 and maintained EVERY DAY using many sources and research.

Thank you, Daniel Dierickx

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

FREE just Click on the LOGO

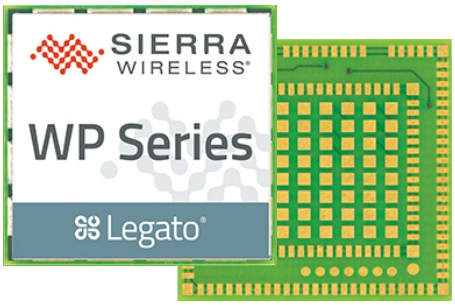
aiworld
IoT World
Telecom COTS World
Broadband Broadcast IoT Convergence
Embedded Systems World
ATCA World

Sierra Wireless announces industry's first global dual-mode LPWA module with integrated application processing and GNSS

AirPrime® WP Series now supports both **LTE-M** (Cat-M1) and **NB-IoT** (Cat-NB1) on a single CF3™ module to simplify design and deployment of innovative LPWA solutions

Vancouver, B.C.-June 28, 2017

Sierra Wireless (NASDAQ: SWIR) (TSX: SW), the leading provider of fully integrated device-to-cloud solutions for the Internet of Things (IoT), today announced the industry's first global, dual-mode Low Power Wide Area (LPWA) cellular modules. The AirPrime® WP77 smart wireless modules simplify LPWA deployments for customers developing products that need to connect to multiple networks where different LPWA technologies are supported.



The WP77 supports both LTE-M (Cat-M1) and NB-IoT (Cat-NB1) with optional 2G fallback, allowing customers to deploy the same device with multiple network operators worldwide. For those deploying in regions where 4G LTE coverage is not as widely available, 2G fallback ensures their devices stay connected to the network.

ABI Research forecasts that cellular LPWA network technologies will begin to see rapid growth from 2018 onward as carriers upgrade their networks in 2017, however, carriers have varying plans and timelines for LTE-M and NB-IoT.

"A module with dual-mode, global coverage will be very attractive for global equipment manufacturers, especially for applications such as telematics, metering, and location tracking, which we expect will lead the way for LPWA volume deployments," said Dan Shey, Managing Director and Vice President at ABI Research.

With the commercialization of LTE-M and NB-IoT LPWA technologies, cellular is now a superior option for many IoT applications that were previously restricted to short-range technologies due to cost and battery life. LPWA technologies combine lower cost, broader coverage and better battery life with globally available and secure cellular networks and will connect millions more things to the Internet.

"With the AirPrime WP77 modules, IoT developers have everything they need in a single module to quickly build low-power connected products that can be deployed anywhere in the world," said Dan Schieler, Senior Vice President and General Manager, Embedded Solutions, Sierra Wireless. "The integrated open source Legato® platform and AirVantage® cloud provide our customers with a proven device-to-cloud architecture to design innovative LPWA solutions that extend the IoT into new applications."

The WP series dramatically simplifies development for secure telematics and gateway applications, providing a dedicated application CPU core running the Linux-based open source Legato application framework. With integrated GNSS for tracking and location-based services, low-power modes, and a comprehensive set of interfaces for connecting sensors and companion chips, including Wi-Fi and Bluetooth, customers can develop multi-service platforms for the transportation market, and use the WP77 for applications requiring low throughput and optimized power performance.

Availability

The AirPrime WP77 is fully compliant with the 3GPP Release 13 standard and compatible with other devices in the WP family, retaining the same footprint, form factor, application framework and Linux distribution. Sierra Wireless AirPrime HL and WP Series modules are the smallest embedded modules (22 x 23 mm) to be completely interchangeable across 2G, 3G, 4G and LPWA technologies. They use the CF3™ form factor, which is footprint compatible across product lines, providing customers with the option to develop smarter by building their connected IoT product or service on a single module. WP77 modules are sampling with lead customers, with general availability in early 2018. For more information, visit http://www.sierrawireless.com/LPWA.

Resources

For more information about LPWA for the IoT, see the LPWA infographic and white paper, LPWA Technologies: Separating Fact from Fiction, and watch the on-demand webinar, The Future of Connectivity for IoT.

To contact the Sierra Wireless Sales Desk, call +1 877-687-7795 or visit http://www.sierrawireless.com/sales.

A Vision for Secure IoT

WHITE PAPER (27 pages)
from CableLabs & Inform[ED] Insights

About CableLabs
Founded in 1988, CableLabs is the Innovation and R&D Lab for the global cable industry.
With a strong focus on innovation, CableLabs develops technologies and specifications for the secure delivery of broadband internet access, video, voice and next generation services. It also provides testing, certification facilities and technical leadership for the industry.
CableLabs' mission is to enable cable operators to be the providers of choice to their customers. CableLabs currently has 59 members across five continents.

About Inform[ED] Insights
The Inform[ED] Insights series addresses major technology developments that have the potential to transform the cable business and society at large.
The cable industry connects and entertains people across the globe, contributing significantly to economic growth and enabling rich discourse in our countries of operation. Inform[ED] Insights will provide leaders across sectors and disciplines with communications technology facts and insights on which to base decisions of significance.

Executive Summary

Download the WHITE PAPER

The rapid proliferation of Internet-connected devices ("Internet of Things" or "IoT") has the potential to transform and enrich our lives and to drive significant productivity gains in the broader economy.

However, the lack of sufficient security in these newly connected devices creates meaningful risk to consumers and to the basic functionality of the Internet. Criminals exploit insecure connected devices to create botnets that launch Distributed Denial of Service ("DDoS") attacks against the Internet infrastructure and online services. As seen this past fall, the Mirai botnet used compromised IP cameras and video recorders to launch the DDoS attack that crippled Dyn, a DNS provider, and impaired Internet access to many popular websites for millions of users.

While Mirai perpetrated one of the most impactful recent DDoS attacks, this will surely not be the last event. Such attacks were once the purview of sophisticated hackers. Now, ready-made DDoS "services" are offered to anyone willing to enter the "Dark Web" with Bitcoin to spend. Ever-increasing broadband capacity, a boon to consumers and the economy, also enables increased volumetric attacks. And, most importantly, the number of attack vectors are growing substantially as IoT devices proliferate – with a doubling or more between 2016 and 2020.

IoT therefore represents the next major axis of growth for the Internet. But, without a significant change in how the IoT industry approaches security, this explosion of devices increases the risk to consumers and the Internet. To reduce these risks, the IoT industry and the broader Internet ecosystem must work together to mitigate the risks of insecure devices and ensure future devices are more secure by developing and adopting robust security standards for IoT devices. Industry-led standards represent the most promising approach to broadly increase IoT security. Given the global and constantly evolving nature of threats, industry must utilize its expertise and reach to develop, adopt, and enforce fundamental IoT security measures.

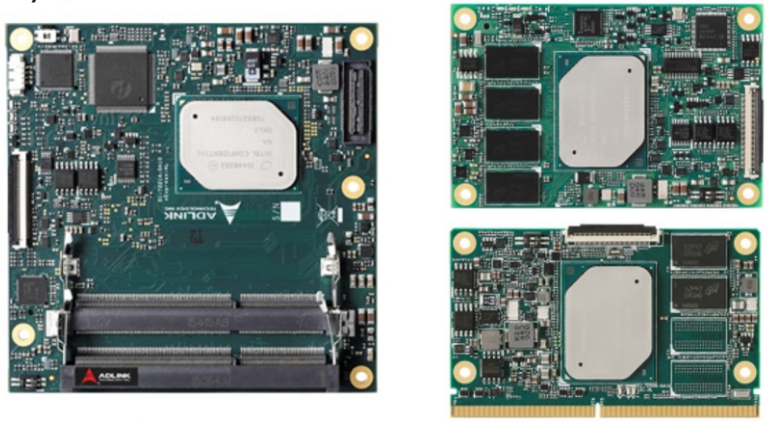
This paper details the technical areas that must be addressed in an IoT security standard. The paper proceeds in three sections: The first provides an overview of the risks posed by insecure IoT to consumers and the Internet. The second highlights the shared responsibility of the entire Internet ecosystem in addressing these risks through mitigation and prevention. The third section details the technical goals of an industryled, standards-based approach as well as the governance goals of the development organization.1 To achieve the needed level of security, an IoT security standard must address: (i) device identity; (ii) authentication, authorization, and accountability (onboarding); (iii) confidentiality; (iv) integrity; (v) availability; (vi) lifecycle management; and (vii) future (upgradable) security. A robust technical standard is necessary but not sufficient. To establish value and credibility in the marketplace, the development organization must be open and balanced, ensure due process and consensus, drive widespread adoption of the standard, address the intellectual property rights of participants, and ensure conformity through strong certification testing and enforcement of the standard.

An industry-led, standards-based approach provides the most viable path to meaningfully increasing the security of IoT devices, given the cross-border, global nature of the challenge and the rapidly evolving nature of the technology and associated threats.

1. The focus of this paper is on consumer/retail single-purpose connected devices (i.e., IoT). The security areas discussed are generally applicable to any Internet-connected device; however, we recognize that in critical or more sensitive applications, additional security features may be warranted.

ADLINK Launches New IIoT Building Blocks Based on Latest Intel® Atom™, Intel® Pentium® and Intel® Celeron® CPU's

New boards and modules provide high efficiency video coding (HEVC) and improved 4K display support, as well as virtualization capabilities and a minimum seven-year lifetime



ADLINK Technology, Inc., a leading global provider of embedded building blocks and application-ready intelligent platforms that enable the Internet of Things (IoT), today announced new computer-on-modules and embedded boards based on the latest Intel® Pentium® N4200 and Intel® Celeron® N3350 processors (codename Apollo Lake) and Intel® Atom™ processor E3900 series (codename Apollo Lake-I). These new offerings take advantage of several improvements over the previous generation of respective Intel® processors, including improved graphics performance with support for Gen 9 LP (18x EUs) and 4K/UHD displays, added virtualization capabilities with full support for Intel® VT-x/VT-d, high-speed DDR3L memory and eMMC 5.0 flash storage.

ADLINK has developed two new COM Express® modules, the Compact Size cExpress-AL and Mini Size nanoX-AL. Both modules offer DDR3L memory up to 1867MHz, with the nanoX-AL supporting a soldered memory capacity range from 2GB to 8GB. In addition to providing three independent display ports that cover DDI/LVDS/optional analog VGA, the cExpress-AL fully utilizes the graphics capabilities enabled through the latest Intel® Atom™ processor and still supports legacy applications. Both modules are cost efficient platforms with rich native I/O support that eliminate the need for an added USB hub, and provide long-life support of at least seven years.

ADLINK's LEC-AL module is based on this year's SMARC 2.0 specification update and offers dual-channel LVDS, 2x MIPI CSI camera interfaces and DDR3L memory up to 1867MHz. The company is also introducing the Q7-AL module based on the Qseven 2.1 specification with fast LPDDR4 memory. All new modules and boards target industrial automation, medical and infotainment applications that require compact, rugged forms factors for harsh, space constrained environments.

Finally, ADLINK's thin Mini-ITX embedded board AmITX-AL-I offers a low profile design, dual DDR3L memory up to 1867MHz, and dual BIOS and Trusted Platform Module (TPM) support. Rich graphics interfaces and I/O includes HDMI, 2x DisplayPort, LVDS/eDP (optional), 7x USB, 6x COM port, dual GbE LAN, PCIe x1, mini-PCIe, 2x SATA 3 and mSATA.

"This latest generation of the Intel® Pentium®, Intel® Celeron® and Intel® Atom™ processors offers several new high-end features that help to lower the overall expense of customer applications requiring high performance computing," said Dirk Finstel, executive vice president of ADLINK's Module Computing Product Segment. "These features include support for up to three independent 4K/UHD displays at 4096x2160@60Hz and added virtualization capabilities, as well as H.265 compression for Internet streaming, which saves bandwidth and lowers communication costs."

All new modules and boards are equipped with ADLINK's Smart Embedded Management Agent (SEMA) to provide access to detailed system activities at the device level, including temperature, voltage, power consumption and other key information, and allow operators to identify inefficiencies and malfunctions in real-time, thus preventing failures and minimizing downtime. ADLINK's SEMA-equipped devices connect seamlessly to our SEMA Cloud solution to enable remote monitoring, autonomous status analysis, custom data collection, and initiation of appropriate actions. All collected data, including sensor measurements and management commands, are accessible any place, at any time via encrypted data connection.

For more information on our new computer-on-module and embedded board offerings based on the latest Intel® Pentium® N4200 and Intel® Celeron® N3350 processors, as well as Intel® Atom™ processor E3900 series. Please visit www.adlinktech.com.

The top 7 Linux IoT projects

By Jon Gold, Senior Writer, Network World | Jun 9, 2017 10:30 AM PT

It's a Linux world, and the rest of computing is just living in it – often literally, thanks to containerization. IoT, in all of its manifold forms, is no exception, and the **Linux Foundation lists these seven projects as the key players in the march of connected open-source systems.** Here's a quick rundown.

Automotive-Grade Linux -- Started: 2012
Key Members: A mix of big car companies (including Mazda, Suzuki, Toyota, Honda, Nissan and Ford), and a diverse array of well-known tech names. Everything from carriers (China Mobile, NTT), silicon makers (Intel, ARM, Nvidia) to electronics powerhouses like LG, Samsung and Panasonic.
+ALSO ON NETWORK WORLD: Experts: The future of IoT will be fascinating and also potentially catastrophic + Top 5 Reasons IoT projects fail
Big Idea: The plan, which is evident from the extensive and wide-ranging list of official project members, is to create an overarching standard for all areas of automotive IoT – everything from telematics to instrumentation to self-driving cars to streaming Netflix for the kids in the back seat. AGL boasts that it's the only such ecosystem that's aiming at all those targets at once.

EdgeX Foundry -- Started: 2017
Key Members: Big names like AMD, Dell/EMC and VMware, operating systems players like Canonical and Linaro, and a host of smaller companies, many of which are related to the cloud in some way.
Big Idea: There are lots of projects and even companies floating around the technology industry with "foundry" in their names, possibly because it sounds industrious and hardworking.
It's arguably more appropriate than most usages here, because EdgeX Foundry is a project devoted to creating open standards for industrial IoT – not all the way down at the sensor level, but ensuring that the hubs, routers and servers that connect them are all speaking the same language.

Tizen -- Started: 2012
Key Members: It was originally a Samsung project, but several other major East Asian tech giants are now members of the executive or advisory boards, including SK Telecom, LG, Huawei, KT & NTT. Oh, also Intel, Orange & Vodafone.
Big Idea: Tizen started life as Samsung's bargaining chip during its sometimes-tense relationship with Google Android on the way to the top of the global smartphone marketplace – Tizen was, ostensibly, a replacement operating system the company could turn to if it decided it didn't like working with Android anymore.
These days, Tizen is likelier to show up on Samsung-built smart watches and TVs than on smartphones (though the company does still have some plans to deploy it there), **but there are some clouds on its horizon**, with the recent revelation of a large number of serious security holes.

Dronecode -- Started: 2014
Key Members: The big players are U.S.-based 3D Robotics and China's Yuneec International, both unmanned aerospace companies. Also on board are Intel, Qualcomm and a raft of lesser-known names related to drones.
Big Idea: You'll be stunned to learn that the big idea is drones – Dronecode aims to deliver an open-source UAV platform, encompassing everything from flight control and autopilot to a custom developer API for "advanced use cases." Dronecode's codebase can be used to create software for custom-built drones, whether you're making them to swoop around and annoy the neighbors or monitor complex atmospheric conditions.

AllJoyn/IoTivity -- Started: 2016 (as joint)
Key Members: Lots of different stakeholders here, including CableLabs, LG, Microsoft, Samsung and Cisco, in addition to the usual players like Intel and Qualcomm. Everyone from the cable ISPs to the wireless providers to smartphone makers to Lowe's is on the Open Connectivity Foundation's membership rolls.
Big Idea: These were originally two different projects, but they merged in 2016 under the aegis of the Linux Foundation's OCF. The idea is to combine IoTivity's discovery and data management tools with AllJoyn's service frameworks and router functionality for a complete, generic IoT platform.

Zephyr Project -- Started: 2016
Key Members: Stop me if you've heard this one: Intel is a platinum member, along with Linaro, NXP Semiconductors and electronic design automation company Synopsys.
Big Idea: Zephyr is a real-time operating system designed to be both highly secure and able to be run on devices with extremely limited computing power – i.e. lots of IoT endpoints. Everything from connected sensors to signage up to the wireless gateway level should be able to run Zephyr, and the current objective seems to be ensuring compatibility across the huge range of devices on which it could be useful.

Yocto Project -- Started: 2010
Key Members: In addition to ubiquitous open-source names like Intel, AMD and Linaro, companies like Juniper Networks, Dell and even Comcast are participants in the Yocto Project.
Big Idea: Yocto is a project designed to help users create customizeable Linux distributions that will run on whatever embedded hardware is available. The core of the project is a development environment that includes tools and guidelines for the creation of those systems, and methods to keep them up to date for any system that a user wants to run them on. The idea is to allow app creators to focus more on core functionality and less on adapting their software to run on particular platforms.

Join the Network World communities on Facebook and LinkedIn to comment on topics that are top of mind.

Introducing Google Cloud IoT Core: for securely connecting and managing IoT devices at scale

By Indranil Chakraborty, Product Manager, Google Cloud

Today (Tuesday, May 16, 2017) we're announcing a new fully-managed Google Cloud Platform (GCP) service called Google Cloud IoT Core. Cloud IoT Core makes it easy for you to securely connect your globally distributed devices to GCP, centrally manage them and build rich applications by integrating with our data analytics services. Furthermore, all data ingestion, scalability, availability and performance needs are automatically managed for you in GCP style.

When used as part of a broader Google Cloud IoT solution, Cloud IoT Core gives you access to new operational insights that can help your business react to, and optimize for, change in real time. This advantage has value across multiple industries; for example:

- **Utilities** can monitor, analyze and predict consumer energy usage in real time
- **Transportation and logistics firms** can proactively stage the right vehicles/vessels/aircraft in the right places at the right times
- **Oil and gas and manufacturing companies** can enable intelligent scheduling of equipment maintenance to maximize production and minimize downtime

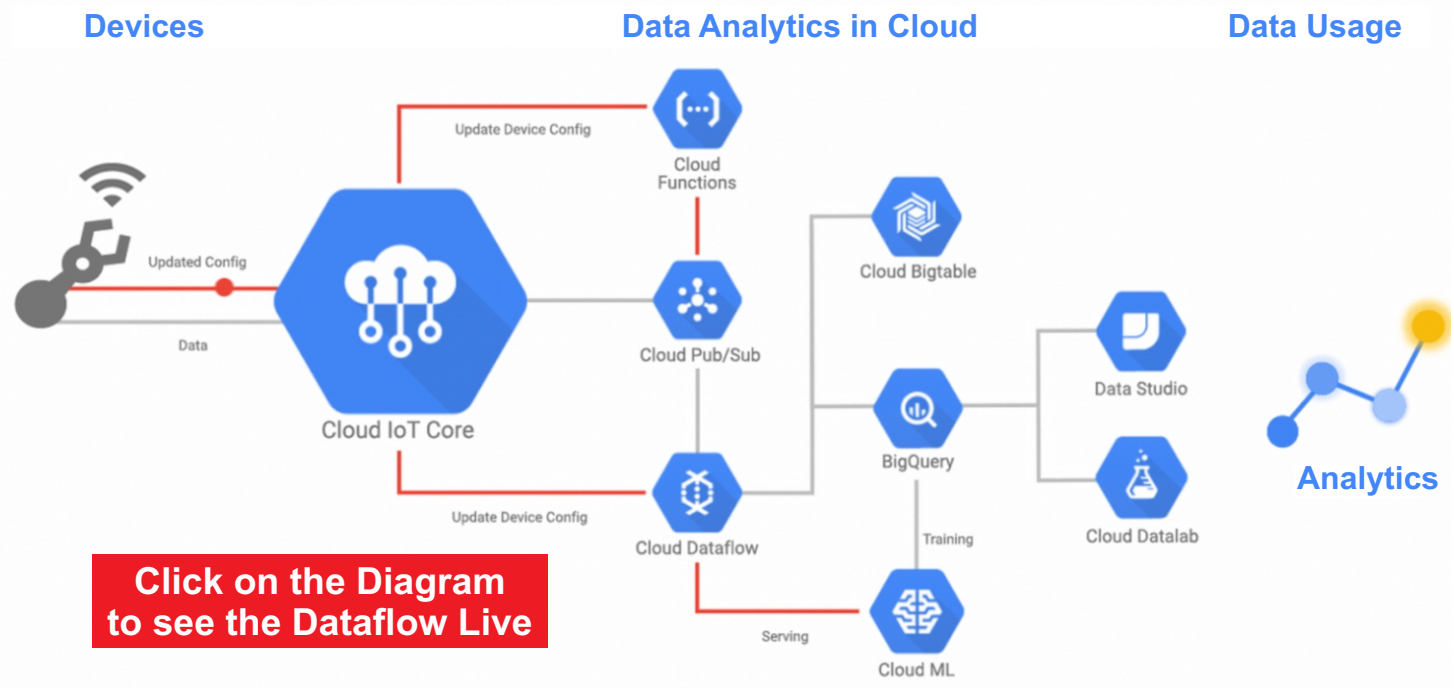
So, why is this the right time for Cloud IoT Core?

About all the things

Many enterprises that rely on industrial devices such as sensors, conveyor belts, farming equipment, medical equipment and pumps — particularly, globally distributed ones — are struggling to monitor and manage those devices for several reasons:

- **Operational cost and complexity:** The overhead of managing the deployment, maintenance and upgrades for exponentially more devices is stifling. And even with a custom solution in place, the resource investments required for necessary IT infrastructure are significant.
- **Patchwork security:** Ensuring world-class, end-to-end security for globally distributed devices is out of reach — or at least not a core competency — for most organizations.
- **Data fragmentation:** Despite the fact that machine-generated data is now an important data source for making good business decisions, the massive amount of data generated by these devices is often stored in silos with a short expiration date, and hence never reaches downstream analytic systems (nor decision makers).

Cloud IoT Core is designed to help resolve these problems by removing risk, complexity and data silos from the device monitoring and management process. Instead, it offers you the ability to more securely connect and manage all your devices as a single global system. Through a single pane of glass you can ingest data generated by all those devices into a responsive data pipeline — and, when combined with other Cloud IoT services, analyze and react to that data in real time.



... to next page

Introducing Google Cloud IoT Core: for securely connecting and managing IoT devices at scale

... from previous page

Key features and benefits

Several key Cloud IoT Core features help you meet these goals, including:

Fast and easy setup and management: Cloud IoT Core lets you connect up to millions of globally dispersed devices into a single system with smooth and even data ingestion ensured under any condition. Devices are registered to your service quickly and easily via the industry-standard MQTT protocol. For Android Things-based devices, firmware updates can be automatic.
Security out-of-the-box: Secure all device data via industry-standard security protocols. (Combine Cloud IoT Core with Android Things for device operating-system security, as well.) Apply Google Cloud IAM roles to devices to control user access in a fine-grained way.
Native integration with analytic services: Ingest all your IoT data so you can manage it as a single system and then easily connect it to our native analytic services (including Google Cloud Dataflow, Google BigQuery and Google Cloud Machine Learning Engine) and partner BI solutions (such as Looker, Qlik, Tableau and Zoomdata). Pinpoint potential problems and uncover solutions using interactive data visualizations, or build rich machine-learning models that reflect how your business works.
Auto-managed infrastructure: All this in the form of a fully-managed, pay-as-you-go GCP service, with no infrastructure for you to deploy, scale or manage.

	Google Cloud IoT Core	DIY
Security by default?	✓ Yes	× No
Easy configuration?	✓ Yes	× No
Native data ingestion?	✓ Yes	× No
Fully managed infrastructure?	✓ Yes	× No
Pay-as-you-go?	✓ Yes	× No

"With Google Cloud IoT Core, we have been able to connect large fleets of bicycles to the cloud and quickly build a smart transportation fleet management tool that provides operators with a real-time view of bicycle utilization, distribution and performance metrics, and it forecasts demand for our customers."
— Jose L. Ugia, VP Engineering, Noa Technologies

Next steps

Cloud IoT Core is currently available as a private beta, and we're launching with these hardware and software partners:

Cloud IoT Device Partners
Actions Semiconductor
Allwinner Technology
ARM
Marvell
Microchip
Intel
Mongoose OS
NXP
Realtek
Sierra Wireless
SOTEC

Cloud IoT Application Partners
Helium
Losant
Mnubo
Tellmeplus

When generally available, Cloud IoT Core will serve as an important, foundational tool for hardware partners and customers alike, offering scalability, flexibility and efficiency for a growing set of IoT use cases. In the meantime, we look forward to your feedback!

MORE: Questions - Feedback and Partners Direct Contact send e-mail to: mgt@e2mos.com

Security and Reliability Are Key in Wireless Networks for Industrial IoT

Ross Yu, Product Marketing Manager
Dust Networks Product Group, Linear Technology

The Industrial Internet of Things (IoT) calls for wireless sensing and control nodes for use in a wide range of applications from factories and industrial process plants to building energy efficiency, smart parking applications and commercial agriculture. In all of these applications, Industrial IoT wireless solutions are expected to operate for many years, often in harsh RF environments and extreme atmospheric conditions. Unlike consumer applications, where cost is often the most important system attribute, industrial applications typically rate reliability and security at the top of the list.

In ON World's global survey of industrial wireless sensor network (WSN) users, reliability and security are the two most important concerns cited.1 This is not surprising, considering that a company's profitability, the quality and efficiency with which they produce goods, and worker safety often relies on these networks. Indeed, Industrial IoT solution providers identified the selection of WSN platform to be pivotal to the success of their wireless Industrial IoT business. This article explains the importance of data reliability and network security in Industrial IoT applications, examines real-life case studies, and discusses key considerations when selecting an Industrial IoT wireless solution.

Data Reliability in a Wireless Sensor Network

WHITE PAPER Click Here includes 2 Case Studies

In an industrial plant or factory, the need for high reliability is well understood since a single missing data point may result in a factory shutdown or safety issues. In the broader set of industrial applications, although the intermittent loss of data packets may be tolerated, extended periods of communications outage are not acceptable. Even a 1% data failure rate is too high, since it translates to 3.65 days per year of unscheduled downtime. Industrial IoT solution providers have noted that one half-day of communications outage would result in irate customers and the cost of an on-site technician visit. If a second such outage were to occur, there is a high likelihood of losing their customer. Therefore, industrial applications demand >99.999% data reliability to overcome the wide variety of RF problems they will likely experience over years of operation.

In order for a wireless network to run virtually maintenance-free for many years, it must be architected with multiple means of overcoming problems. One general principle in designing a network for reliability is redundancy, where failover mechanisms for likely problems enable systems to recover without data loss. In a wireless sensor network, there are two basic opportunities to harness this redundancy. First is the concept of spatial redundancy, where every wireless node has at least two other nodes with which it can communicate, and a routing scheme that allows data to be relayed to either node, but still reach the intended final destination. A properly formed mesh network—one in which every node can communicate with two or more adjacent nodes—enjoys higher reliability than a point-to-point network by automatically sending data on an alternate path if the first path is unavailable.

The second level of redundancy can be achieved by using multiple channels available in the RF spectrum. The concept of channel hopping ensures that pairs of nodes can change channels on every transmission, thereby averting temporary issues with any given channel in the ever changing and harsh RF environment typical of industrial applications. Within the IEEE 802.15.4 2.4GHz standard, there are fifteen spread spectrum channels available for hopping, affording channel hopping systems much more resilience than non-hopping (single channel) systems. There are several wireless mesh networking standards that include this dual spatial and channel redundancy known as Time Slotted Channel Hopping (TSCH), including IEC62591 (WirelessHART) and the forthcoming IETF 6TiSCH standard.2 These mesh networking standards, which utilize radios in the globally available unlicensed 2.4GHz spectrum, evolved out of work by Linear Technology's Dust Networks® group, which pioneered the use of TSCH protocols on low power, resource constrained devices since 2002 with SmartMesh® products.

While TSCH is an essential building block for data reliability in harsh RF environments, the creation and maintenance of the mesh network is key for continuous, problem-free multi-year operation. Over its lifetime, an industrial wireless network will be subject to vastly different RF challenges and data transmission requirements. Therefore, the final ingredient required for wire-like reliability is intelligent network management software that dynamically optimizes the network topology, continuously monitoring link quality to maximize throughput despite interference or changes to the RF environment.

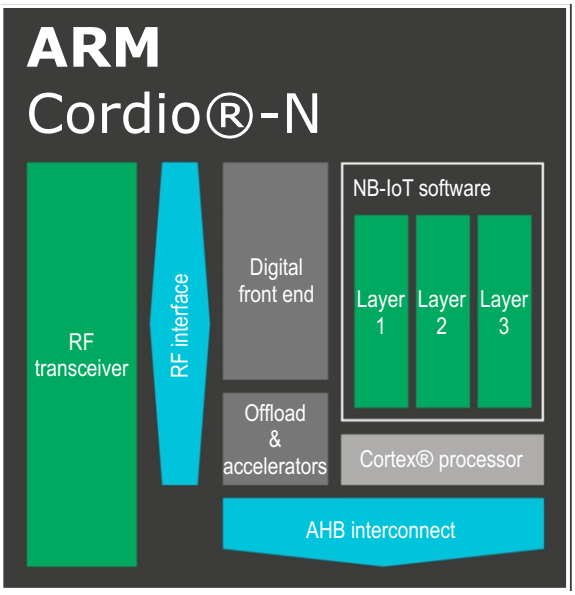
1 Industrial Wireless Sensor Networks: Trends and Developments, https://www.isa.org/standards-publications/isa-publications/intechmagazine/2012/october/web-exclusive-industrial-wireless-sensornetworks/
2 6TiSCH Wireless Industrial Networks: Determinism Meets IPv6: Maria Rita Palattella, Pascal Thubert, Xavier Vilajosana, Thomas Watteyne, Qin Wang, and Thomas Engel. Published in: Communications Magazine, IEEE (Volume: 52, Issue: 12).

Enabling mass IoT connectivity as ARM partners ship 100 billion chips

The ARM business model has inspired innovators, entrepreneurs, academics and now – the cumulative deployment of 100 billion chips, half of which shipped in the last four years. It is an amazing achievement but success does not belong to ARM alone, rather it is testament to the power of partnership.

And if partnership can create and deploy 100 billion chips, why not a trillion or more? That is our target, seeing a trillion connected devices deployed over the next two decades. And for that to happen, we must think carefully about the ecosystem and infrastructure required to support such a vast quantity of data-driven products.

NarrowBand-IoT



Connecting a trillion devices requires a range of enabling technologies. In the home that may be Wi-Fi or Bluetooth low energy. For devices operating remotely, in power-constrained environments and sending infrequent amounts of little data, there are new cellular-based technology standards delivered by the 3GPP Release 13 in 2016. That included NarrowBand-IoT (NB-IoT) and LTE Cat M1. We expect NB-IoT, an ultra-low-power wide-area connectivity (LPWAN) standard, to be a key enabler of a broad range of IoT applications and that is why we announced ARM Cordio-N NB-IoT radio technology last week. With broadly available IP from ARM, any chip designer will be able to integrate NB-IoT functionality into a product and reduce overall system costs.

Tadashi Iida, vice president and head of the Mobile Technology Division at SoftBank Corp agrees: "The industry is planning a complex network transformation to cope with the weight of devices that will connect over the next two decades."

He adds: "We will see advanced and efficient compute, security, storage, and connectivity from the edge of the system to the Cloud. NB-IoT will play an important role in this transformation as it lays a path towards the massive machine communications needs of 5G. ARM's licensable IP, ARM Cordio-N NB-IoT modem will help hasten this path as it will enable developers to bring products to market faster, and at scale."

Built for purpose

For me, the beauty of NB-IoT is that it will enable the smallest embedded edge devices to send tiny amounts of data using licensed spectrum while being so efficient that devices may last for ten years or more on a battery. Along with offering reliable quality of service, the standard is highly attractive to mobile network operators as it is relatively inexpensive to deploy on their existing cellular networks.

Ryan Sullivan, vice president of Product Engineering & Development at Sprint, also believes cellular standards will unlock the IoT at scale: "Delivering secure connectivity will be mission critical for a wireless Operator requiring a robust and holistic communication and data ecosystem. ARM's IP technology and ecosystem offers a path to accelerate cellular IoT adoption by delivering a secure solution certified at the chip. By utilizing the ARM ecosystem, we expect improved costs and time-to-market that will drive innovation for IoT and Enterprise solutions."

Design to delivery - fast

Our aim now is to achieve network pre-certification of ARM Cordio-N NB-IoT IP. This would allow our chip and OEM partners to build secure connected products from the ground up to be secure and resilient enough to run on cellular networks. If we succeed, along with our operator partners, we will have made it far easier and cheaper for developers to get to market. For anyone, trying to get a new device up and running as fast as possible out of the box, this will be a huge plus.

This is all part of ARM's ultimate vision; to transform technology experiences through a total computing approach that creates a vast network of securely-connected smart devices that enhance every aspect of peoples' lives. Today, alongside our 1,100 partners, we celebrate 100 billion ARM-based chips shipped, but that is only the start.

Download our free white paper 'NB-IoT: Connecting the IoT with ARM' for more on how NB-IoT will unlock long range IoT connectivity at scale.

Simon Segars, CEO, ARM Holdings plc

How to update a billion devices in field

By Bee Hayes-Thakore

ARM was for the first time at Hannover Messe (April 24-28, 2017), addressing the Digital Factory businesses from around the world and exploring the challenges and opportunities that Industrial IoT (IIoT) brings. ARM experts were showcasing how our unique mbed Cloud technology can enable secure device management to drive down costs in the industrial operations that increasingly utilize IoT products.

In the last 12 months, we have seen a transformation in how the IoT is viewed by business: More than 50 percent of senior leaders report that IoT is an important part of their business strategy, and many companies are now rolling out IoT services.

In the next five years the European IIoT market is expected to be worth $629 billion. To unlock this potential, ARM has developed technology that will reduce the cost of scaling-out secure IoT systems.

One of the major challenges facing IoT deployment is addressing the operational needs of devices through their lifecycle, particularly in ensuring that devices have the correct software installed, that firmware is protected against security vulnerabilities, and that as new devices are installed, application and functionality updates are managed.

Understanding the last mile: Will the update reach?

In the industrial context, a remote device may be embedded in a harsh environment where access is limited. It may be buried next to a mast in a weatherproof case; it may require technicians to travel hundreds of miles to repair. These devices may be deployed across a diverse network topology at the edge. Mechanisms designed for previous networked equipment may even be too constrained for IoT devices. When we discuss the needs of teams responsible for managing and updating IoT devices, the success and return on investment of IoT deployments depends on addressing questions like:

- How can I update my devices?
- What happens if a thunderstorm hits?
- What if there is a power outage part way through the update that corrupts info on the device?

ARM did showcase how easy it is to administer secure, reliable, fail-safe updates with the new mbed Cloud device management solution. Most solutions allow developers to bring their own mechanism to build firmware and software updates into IoT deployments. mbed Cloud Update delivers all of the required components in a simple service to make secure remote updates possible.

Secure: Offering authenticity, integrity and confidentiality protection

Fail-safe: Update campaigns protected during power failures and no rollback

Campaign tracking: Accurate campaign tracking reducing maintenance costs

Conditional control: Rules to avoid interrupting critical device operations

... to next page

How to update a billion devices in field

... from previous page

Moving trust closer to the edge brings cost savings

ARM mbed Cloud Update works in conjunction with a device-side secure bootloader that OEMs can use to ensure that the firmware update being administered is validated and authenticated before it is loaded on the device.

Security is a cornerstone of mbed Cloud Update and the enhanced service secures delivery of firmware over multiple infrastructures and protocols, which is essential for connected industrial operations. As security elements are independent of transport protocol, the service supports a wider range of protocols. It also supports caching in the cloud environment. This enables users to bring update capability across a range of networks whilst saving money and improving flexibility. The service will also support encrypted update packages. This can be used to protect IP or to observe security licensing restrictions.

Further, updates across large deployments scaling millions and billions of devices can take a long time. Thunderstorms may not always be the culprit, but power fluctuations or power outages through long update campaigns are all too common. mbed Cloud Update is designed to support practical considerations for remote throttling and rollback protection preventing devices from being accidentally or maliciously rolled back to an older, more vulnerable firmware version.

Look for tried and tested pathways to production

Lower costs are realized by reducing field call-outs for devices that haven't updated as desired in the campaign. Being able to troubleshoot devices can save hundreds, if not thousands, of dollars for each time someone has to be sent into the field to access devices. Blueprints and approaches for such update campaigns are well established and can be tuned to address IoT requirements with the right partner and ecosystem to accelerate efforts.

Bee Hayes-Thakore is director of marketing programs for IoT at ARM.

ARM invests in the future of IoT connectivity

ARM acquires Swedish Mistbase and English NextG-Com to bring NB-IoT compliant technology to ARM-based chips

The IoT is made up by billions of connected devices – which will serve a huge range of application needs. From single-sensor devices regulating and monitoring factory production flows to intelligence stitched into a city's arteries to tune streetlights to the presence of people, vehicle traffic and weather conditions.

And as ARM wireless business general manager Paul Williamson points out in a blog post; "Despite the incredible range of use cases there are two non-negotiable elements that must be architected into the system's heart – security and low power. Security because the system must be trusted, low power because energy equals cost."

Looking back a few months there was an industry breakthrough on both fronts during the summer – the NarrowBand-IoT (NB-IoT), a new low power wide area connectivity standard, was approved. It is seen as the standard that will unlock long range IoT connectivity at scale as mobile network operators only have to upgrade their existing LTE systems to make it work.

"The question for me in leading ARM's wireless business was how to move quickly to enable our partners to design NB-IoT compliant products. This week we made significant progress on that by acquiring Mistbase and NextG-Com for their specialist engineering expertise in software and hardware IP that meets the new NB-IoT standard" Paul Williamson writes in the blog post.

Mistbase is based in Lund, Sweden, and provides a complete NB-IoT physical layer implementation solution. NextG-Com is based in London, England, and offers a complete layer two and three software stack for NB-IoT. Both teams have experience in cellular standards and IP development and are already working together to provide integrated solutions.

"The acquisitions expand the ARM portfolio of IoT connectivity which already includes established short range Bluetooth 5 and 802.15.4 Cordio products. By providing complete connectivity IP options of short range PAN (Personal Area Network) and long range NB-IoT connectivity, ARM is enabling its partners to address any class of IoT application from the smart city and smart home, to the factory and farm," Paul Williamson states.

Published by our colleagues in Sweden: Evertiq New Media AB http://evertiq.com