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

July-August 2016

Headlines:

- Popular IoT Forecast of 50 Billion Devices by 2020 Is Outdated
- ARM at the heart of Industrial IoT
- The 7 Biggest Mistakes Manufacturers Make When Launching IoT Products
- Real World Security and the Internet of Things *****
- Open standards in IoT deployments would accelerate growth by 27% and reduce deployment costs by 30%
- congatec introduces highly flexible IoT gateway Qseven-based
- Pycom Collaborates with Sigfox to bring out The SiPy in October 2016

Adlink IoT Gateway Line Expands Support for Intel® IoT Gateway Technology

Intel® Quark™
Intel® Atom™
Intel® Core™
processor-based
models deliver
scalable computing
solutions for a variety
of Industrial
IoT applications

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

ARM AT THE HEART OF THE INDUSTRIAL INTERNET OF THINGS

London, England; July 18, 2016; Colin Barnden, Principal Analyst, Semicast Research Ltd

According to the latest analysis by Semicast Research, the number of devices available to be connected to the Industrial Internet of Things (IIoT) is forecast to grow to almost 2.5 billion annually in 2021, from about 1.2 billion in 2015, a growth rate of almost fifteen percent. Similarly, the total available market for electronics equipment suitable to be connected to the IIoT is forecast to grow to over USD 930 billion, from USD 675 billion over the same period, a growth rate of about six percent.

Semicast has covered the market for industrial electronics and semiconductors since 2006 and views the sector as a series of markets within a market, each with its own trends and suppliers. This arguably makes it the most complex sector for electronics and semiconductor vendors to understand and support. Semicast defines the industrial electronics market to include traditional areas such as factory automation, motor drives, lighting, building automation, surveillance, test & measurement and power & energy, as well as medical and industrial transportation equipment such as construction and mining; aerospace & defense is excluded. It is Semicast's view that the IIoT can be broadly described as intelligence and connectivity being added to ever smaller, distributed, remote industrial devices. This includes obscure, somewhat dull products, such as pressure measurement, proximity sensors and motion detectors, which offer none of the glamor and allure of smart watches or wearables, but which nonetheless are manufactured in volumes of tens of millions of units per year.

Unlike wearables and other "smart things", demand for these devices is established and their market sizes known; the trend of IIoT is for more of them to be intelligent and connected. This intelligence and connectivity increasingly comes from the addition of sub-$1 32-bit microcontrollers, together with wireless communications such as 6LoWPAN, Bluetooth/BLE, LoRa, NFC, Sub-1/2.4 GHz, Wi-Fi and ZigBee. Colin Barnden, Principal Analyst at Semicast Research and study author, commented "These intelligent, connected, industrial devices generate the Little Data which has never previously been captured, to be processed locally or fed straight to the Cloud for Big Data analytics, thus creating the IIoT of smart buildings, cities, factories, grid, medical, payment and security."

UK-based ARM Holdings (ARM) dominates the technology and intelligence powering the IIoT and its leadership in this market helps explain Softbank's announcement to buy ARM for USD 32 billion on July 18. Using data from Semicast's 2016 Industrial/Medical Electronics & Semiconductors Service, ARM's market share for 32-bit microcontrollers in industrial and medical applications is estimated at about 80% when measured in units, while for microprocessors it is about 50%. Intel currently dominates Big Data processing at the core of the IIoT, but ARM is steadily building its share in the Little Data analytics at the network edge.

Barnden summed up "Softbank's purchase of ARM seems a little like buying ExxonMobil to fill your gas tank. Only time will tell if this was a smart move by Softbank, but at a premium of more than 40% of the previous closing price, ARM's shareholders will be celebrating already".

Editor Note -- I selected this interesting article from Colin and would like to make a comment on the acquisition. Indead **Softbank** (a Japanese leading Telco Service Provider) has a very different activity than **ARM** (CPU IP provider), it is not like Intel buying Altera, two very complementary chip suppliers.

But: do you remember **P.A. Semi** acquired by **Apple** in April 2008 for USD 278 million
P.A. Semi (originally Palo Alto Semiconductor) was a fabless semiconductor company founded in Santa Clara, California in 2003 by **Daniel W. Dobberpuhl** who was previously the lead designer for the **DEC** Alpha 21064 and StrongARM processors. **Apple** CEO **Steve Jobs** said that the acquisition was meant to add the talent of P.A. Semi's engineers to Apple's workforce and help them build custom chips for the iPod, iPhone.
I think Softbank/ARM is something similar, Softbank has clearly announced that they will play a major role in the IoT business in terms of services and products. I believe that ARM will provide Softbank with a dramatic "Competitive Advantage" like P.A. Semi did for Apple.

Secondary effect: when Apple bought P.A. Semi they said that supply to current customers will continue, but that was not for a long time and there were some bad consequences. For example **XES** (**Extreme Engineering Solutions**, a US-based leading embedded computing board manufacturer) designed a very high performance and very low power **ATCA*** CPU board back in 2007 (XES Press Release June 18, 2007), unfortunately XES had to decide to stop the business with this product because "End of Life" of the chip. Very sad because this ATCA board was certainly one of the most beautiful product in that range (2 x 9 Cores in 2007), very high performance and very low power, still a challenge in Telecom. I still have a nice picture and all doc's.
So let's put a note in our **Outlook for September 21st 2017** and the next 3 years, as you know "nothing is holder than the news of last night"

*ATCA = **Advanced Telecom Computing Architecture**, the ATCA Platforms are deployed in all the World's major networks (is the brain of many 4G / LTE systems). **Huawei** was an early adopter of ATCA, they started buying ATCA Servers but moved rapidly to own R&D and manufacturing. ATCA was a dominant factor to bring Huawei to the N° 1 market position today.

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

Our 4 e-magazines - FREE Worldwide

Telecom COTS World Broadband Broadcast IoT Convergence www.telecomcots.com
IoT World www.iotworld.be
Embedded Systems World www.emb-sys-world.com
ATCA World Advanced Telecom Computing Architecture www.atcaworld.com

Publication: e2mos www.e2mos.com **Contact:** mgt@e2mos.com

ADLINK IoT Gateway Line Expands Support for Intel® IoT Gateway Technology

Intel® Quark™ , Intel® Atom™ and Intel® Core™ processor-based models deliver scalable computing solutions for a variety of Industrial IoT applications

San Jose, CA, June 21, 2016 – ADLINK Technology, a leading global provider of embedded building blocks, intelligent gateways and cloud/fog computing solutions that enable the Industrial Internet of Things (IIoT), announces the release of three ADLINK IoT gateway models supporting Intel® IoT Gateway Technology. The MXE-110i, MXE-202i, and MXE-5400i, based on the Intel® Quark™, Intel® AtomTM, and Intel® Core™ processors, respectively, further expand the scope of ADLINK's IoT gateway-based scalable computing platforms. From energy-saving applications to intelligent analytics, ADLINK's IoT gateways supporting Intel® IoT Gateway Technology provide the ideal IoT-ready industrial platforms for a wide variety of applications.

Intel® IoT Gateway Technology enables development of intelligent gateways, which are critical to connecting systems with next-generation intelligent infrastructures and increasing business value for a world of applications. The ADLINK IoT Gateway product line, fully supported by Intel® IoT Gateway Technology, with integrated Wind River® Intelligent Device Platform XT, and McAfee Embedded Control, is available for Intel® IoT Gateway Software Suite, Intel® IoT Gateway Pro Software Suite, and Intel® IoT Gateway Pro Pilot Software Suite.

"We understand customers require an application-ready solution to tackle the complexity of IIoT infrastructure. We're happy to leverage Intel Gateway Technology to provide seamless connectivity between devices and the cloud, ensuring the interoperability of edge devices through an open architecture enabling rapid application and service, all to successfully equip new connected applications with minimum effort," said Roy Wan, general manager of ADLINK's Measurement and Automation Product Segment.

"A key motivator in the adoption of IIoT functionality is the potential to unlock knowledge from their data," said Rose Schooler, vice president IoT Strategy and Technology at Intel. "Because ADLINK's full spectrum of IoT gateway platforms utilize the latest version of Intel IoT Gateway Technology, developers will be able to utilize new enhancements designed to help prototype and develop IoT applications more quickly than ever."

The latest version of Intel® IoT Gateway Technology enables enhanced user interface, security, scalability, interoperability, and manageability, as well as support for a wider variety of fieldbus communication protocol, including Modbus (RTU/Ethernet), BACNet, CAN for industrial applications, Exegin, Zigbee, Open Z-Wave, and 6lowpan empowering smart buildings. Other features include support for MQTT, Bluetooth/BLE, CoAP, XMPP device-to-cloud protocol, as well as AllJoyn and IoTivity (open source software framework) to enable seamless device-to-device connectivity.

New additions to ADLINK's IoT gateway product line include the MXE-110i, MXE-202i, and MXE-5400i. The MXE-5400i, based on Intel® Core™ i3, Intel® Core™ i5, and Intel® Core™ i7 processors. These processors deliver exceptional performance and manageability, optimized connectivity, and rugged construction for mission-critical applications. The gateway performs dependably under an extended operating temperature range (from –20°C to 70°C with industrial SD card), making it the optimal solution for outdoor intelligent transportation, digital surveillance systems, and industrial automation applications. The MXE-202i gateway, powered by the Intel® Atom™ processor E3826, features two processing cores with an SoC design, delivering the computing performance needed to handle the flow of data from sensors, while power-efficient enough to perform reliably in a fanless enclosure. Finally, the MXE-110i gateway, based on the Intel® Quark™, is suitable for applications requiring enhanced energy efficiency, such as smart agriculture, smart factory, and automated building environments.

For more information on our IoT gateways, please visit:
http://www.adlinktech.com/Industrial-PCs-Fanless-Embedded-PCs/IoT-Gateway.php
For more information on ADLINK, please visit: www.adlinktech.com

About ADLINK

ADLINK Technology is enabling the Internet ofThings (IoT) with innovative embedded computing solutions for edge devices,intelligent gateways and cloud services. ADLINK's products are application-ready for industrial automation, communications, medical, defense, transportation, and infotainment industries. Our product range includes motherboards, blades, chassis, modules, and systems based on industry standard form factors, as well as an extensive line of test & measurement products, smart touch computers, displays and handhelds that support the global transition to always connected systems. Many products are Extreme Rugged™, supporting extended operating temperature ranges, and MIL-STD levels of shock and vibration.

Open standards in IoT deployments would accelerate growth by 27% and reduce deployment costs by 30%

White Paper (16 pages) **Machina Research** sponsored by **InterDigital** - May 2016

Machina Research forecasts that the growth of the Internet of Things (IoT) will be substantial, but standardization could lead to even more rapid growth. This White Paper examines the impact of a fragmented versus a standards-based approach to the IoT as it relates to the emergence of smart cities. Smart cities were selected specifically because they are a microcosm of the IoT; deployments inevitably touch several separate vertical domains, and involve multiple parties, and diverse IT systems. They are therefore a good illustration of the effects of fragmentation and of the relative merits of various means of addressing it.

The White Paper is aimed at city authorities as well as their technology partners, since the development of smart cities is usually based on a hybrid approach of public-private partnering and planning1. InterDigital, the sponsor of this White Paper, supports and promotes open standards through an open platform for IoT interconnectivity and the controlled sharing of data and analysis.

This White Paper addresses the following questions:

- What is the opportunity cost, or difference, between standard-based and non-standardised environments, as it relates to smart cities?
- What is the cost impact to city managers of ongoing inefficiencies that non-standards-based approaches are causing?
- What impact will the use of non-standards-based approaches cause in terms of not achieving the potential of mass scale for IoT interoperability?
- How are operators affected by not achieving the potential of standardization of IoT in smart cities, as greater IoT revenues depend on increasing volumes of IoT traffic to carry and process?

The smart cities domain illustrates the importance of standards in enabling deployment and ensuring best practice; but as a complex and multi-dimensional vertical that crosses boundaries between public and private sectors it also shows the challenges inherent in moving towards standards in an environment characterised by multiple systems, vendors, verticals and stakeholders. For this reason we have chosen to use it to demonstrate in a quantitative way the impact of a standards-based approach. DOWNLOAD THE WHITE PAPER

Real World Security and the Internet of Things *****

August 2016 – By Bruce Schneier

Disaster stories involving the Internet of Things are all the rage. They feature cars (both driven and driverless), the power grid, dams, and tunnel ventilation systems. A particularly vivid and realistic one, near-future fiction published last month in New York Magazine, described a cyberattack on New York that involved hacking of cars, the water system, hospitals, elevators, and the power grid. In these stories, thousands of people die. Chaos ensues. While some of these scenarios overhype the mass destruction, the individual risks are all real. And traditional computer and network security isn't prepared to deal with them.

Classic information security is a triad: confidentiality, integrity, and availability. You'll see it called "CIA," which admittedly is confusing in the context of national security. But basically, the three things I can do with your data are steal it (confidentiality), modify it (integrity), or prevent you from getting it (availability).

So far, Internet threats have largely been about confidentiality. These can be expensive; one survey estimated that data breaches cost an average of $3.8 million each. They can be embarrassing, as in the theft of celebrity photos from Apple's iCloud in 2014 or the Ashley Madison breach in 2015. They can be damaging, as when the government of North Korea stole tens of thousands of internal documents from Sony or when hackers stole data about 83 million customer accounts from JPMorgan Chase, both in 2014. They can even affect national security, as in the case of the Office of Personnel Management data breach by -- presumptively -- China in 2015.

On the Internet of Things, integrity and availability threats are much worse than confidentiality threats. It's one thing if your smart door lock can be eavesdropped upon to know who is home. It's another thing entirely if it can be hacked to allow a burglar to open the door -- or prevent you from opening your door. A hacker who can deny you control of your car, or take over control, is much more dangerous than one who can eavesdrop on your conversations or track your car's location.

With the advent of the Internet of Things and cyber-physical systems in general, we've given the Internet hands and feet: the ability to directly affect the physical world. What used to be attacks against data and information have become attacks against flesh, steel, and concrete.

Today's threats include hackers crashing airplanes by hacking into computer networks, and remotely disabling cars, either when they're turned off and parked or while they're speeding down the highway. We're worried about manipulated counts from electronic voting machines, frozen water pipes through hacked thermostats, and remote murder through hacked medical devices. The possibilities are pretty literally endless. The Internet of Things will allow for attacks we can't even imagine. **... to Next Page**

The increased risks come from three things: software control of systems, interconnections between systems, and automatic or autonomous systems. Let's look at them in turn:

Software Control. The Internet of Things is a result of everything turning into a computer. This gives us enormous power and flexibility, but it brings insecurities with it as well. As more things come under software control, they become vulnerable to all the attacks we've seen against computers. But because many of these things are both inexpensive and long-lasting, many of the patch and update systems that work with computers and smartphones won't work. Right now, the only way to patch most home routers is to throw them away and buy new ones. And the security that comes from replacing your computer and phone every few years won't work with your refrigerator and thermostat: on the average, you replace the former every 15 years, and the latter approximately never. A recent Princeton survey found 500,000 insecure devices on the Internet. That number is about to explode.

Interconnections. As these systems become interconnected, vulnerabilities in one lead to attacks against others. Already we've seen Gmail accounts compromised through vulnerabilities in Samsung smart refrigerators, hospital IT networks compromised through vulnerabilities in medical devices, and Target Corporation hacked through a vulnerability in its HVAC system. Systems are filled with externalities that affect other systems in unforeseen and potentially harmful ways. What might seem benign to the designers of a particular system becomes harmful when it's combined with some other system. Vulnerabilities on one system cascade into other systems, and the result is a vulnerability that no one saw coming and no one bears responsibility for fixing. The Internet of Things will make exploitable vulnerabilities much more common. It's simple mathematics. If 100 systems are all interacting with each other, that's about 5,000 interactions and 5,000 potential vulnerabilities resulting from those interactions. If 300 systems are all interacting with each other, that's 45,000 interactions. 1,000 systems: 12.5 million interactions. Most of them will be benign or uninteresting, but some of them will be very damaging.

Autonomy. Increasingly, our computer systems are autonomous. They buy and sell stocks, turn the furnace on and off, regulate electricity flow through the grid, and -- in the case of driverless cars -- automatically pilot multi-ton vehicles to their destinations. Autonomy is great for all sorts of reasons, but from a security perspective it means that the effects of attacks can take effect immediately, automatically, and ubiquitously. The more we remove humans from the loop, faster attacks can do their damage and the more we lose our ability to rely on actual smarts to notice something is wrong before it's too late.

We're building systems that are increasingly powerful, and increasingly useful. The necessary side effect is that they are increasingly dangerous. A single vulnerability forced Chrysler to recall 1.4 million vehicles in 2015. We're used to computers being attacked at scale -- think of the large-scale virus infections from the last decade -- but we're not prepared for this happening to everything else in our world.

Governments are taking notice. Last year, both Director of National Intelligence James Clapper and NSA Director Mike Rogers testified before Congress, warning of these threats. They both believe we're vulnerable.

This is how it was phrased in the DNI's 2015 Worldwide Threat Assessment: "Most of the public discussion regarding cyber threats has focused on the confidentiality and availability of information; cyber espionage undermines confidentiality, whereas denial-of-service operations and data-deletion attacks undermine availability. In the future, however, we might also see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e. accuracy and reliability) instead of deleting it or disrupting access to it. Decision-making by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving."

The DNI 2016 threat assessment included something similar: "Future cyber operations will almost certainly include an increased emphasis on changing or manipulating data to compromise its integrity (i.e., accuracy and reliability) to affect decision making, reduce trust in systems, or cause adverse physical effects. Broader adoption of IoT devices and AI -- in settings such as public utilities and healthcare -- will only exacerbate these potential effects."

Security engineers are working on technologies that can mitigate much of this risk, but many solutions won't be deployed without government involvement. This is not something that the market can solve. Like data privacy, the risks and solutions are too technical for most people and organizations to understand; companies are motivated to hide the insecurity of their own systems from their customers, their users, and the public; the interconnections can make it impossible to connect data breaches with resultant harms; and the interests of the companies often don't match the interests of the people.

Governments need to play a larger role: setting standards, policing compliance, and implementing solutions across companies and networks. And while the White House Cybersecurity National Action Plan says some of the right things, it doesn't nearly go far enough, because so many of us are phobic of any government-led solution to anything. The next president will probably be forced to deal with a large-scale Internet disaster that kills multiple people. I hope he or she responds with both the recognition of what government can do that industry can't, and the political will to make it happen.

About the author - I've been writing about security issues on my blog since 2004, and in my monthly newsletter since 1998. I write books, articles, and academic papers. Currently, I'm the Chief Technology Officer of Resilient, an IBM Company, a fellow at Harvard's Berkman Center, and a board member of EFF. **More** about Bruce Schneier

The 7 Biggest Mistakes Manufacturers Make When Launching IoT Products

WHITE PAPER

The 7 Biggest Mistakes Manufacturers Make When Launching IoT Products From Ayla Networks

Introduction

The path to creating successful connected products is littered with road kill. Many industry leading manufacturers stumble getting their discrete products connected and and creating meaningful solutions. Without deep insight into all the potential pitfalls of launching connected products for the IoT, manufacturers are likely to make critical mistakes. Some of these mistakes can be extremely costly, in money, time, and frustration.

To help you take a smoother path to your connected products—and to prevent a "Fire, Aim, Ready" approach—here are the 7 biggest mistakes when launching into the IoT market, and how to avoid them.

Mistake #1
Designing an IoT solution without identifying a specific use case

Mistake #2
Choosing hardware before choosing your IoT cloud

Mistake #3
Failing to budget enough time for the project

Mistake #4
Overengineering the first version of your IoT product

Mistake #5
Neglecting to make OTA (over-the-air) communications a priority

Mistake #6
Doing too little field testing

Mistake #7
Approaching the IoT like a new feature rather than a whole new category

Download the White Paper Click Here

Ayla Networks

Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated

By Amy Nordrum, Associate Editor at IEEE Spectrum
Posted 18 Aug 2016 | 13:00 GMT

If you follow discussions about the Internet of Things, you've probably heard this stunning prediction at least once: The world will have 50 billion connected devices by 2020. Ericsson's former CEO Hans Vestburg was among the first to state it in a 2010 presentation to shareholders. The following year, Dave Evans, who worked for Cisco at the time, published the same prediction in a white paper.

Today, that figure has arguably done more than any other statistic to set sky-high expectations for potential IoT growth and profits. Remarkably, those projections weren't even close to the highest of the time—in 2012, IBM forecasted 1 trillion connected devices by 2015. "The numbers were getting kind of crazy," recalls Bill Morelli, a market research director for IHS Markit.

Now it's 2016, and we're nowhere near 1 trillion IoT devices, or even 50 billion for that matter. The current count is somewhere between Gartner's estimate of 6.4 billion (which doesn't include smartphones, tablets, and computers), International Data Corporation's estimate of 9 billion (which also excludes those devices), and IHS's estimate of 17.6 billion (with all such devices included).

Since they first made their projections, both Ericsson and Evans have lowered their expectations from 50 billion for 2020: Evans, who is now CTO of Stringify, says he expects to see 30 billion connected devices by then, while Ericsson figures on 28 billion by 2021. Other firms have adopted similar tones: IHS Markit projects 30.7 billion IoT devices for 2020, and Gartner expects 20.8 billion by that time (excluding smartphones, tablets, and computers). Lastly, IDC anticipates 28.1 billion (again, not counting those devices).

Meanwhile, the popular 50 billion figure continues to be widely cited. Even Evans is a bit surprised by its lasting power. "I think people do tend to latch onto numbers that seem really hard to fathom," he says. "Fifty billion is pretty staggering."
Forecasting the future is no easy task, and there's nothing unusual or wrong about analysts and companies revising their projections. However, IoT forecasts are especially large with significant variability among firms and over time, skewing tens of billions of units in either direction.

At the same time, any market with such potential girth dazzles entrepreneurs and investors. For comparison, 18.6 billion microcontrollers were shipped in 2014, and 10.4 billion RFID tags will be shipped this year. Given the forecasts, IoT is expected to top them all. "I don't think we've seen this type of market size before, to be honest," says Vernon Turner, a senior IoT analyst for IDC.

Peter Middleton, a research director at Gartner involved in the firm's IoT forecasts, says future IoT projections are intended to create "market efficiency," helping companies make smart choices about whether they should enter a new area and informing venture capitalists as they decide where to place their investments. Earlier this week, Intel executive Venkata Renduchintala emphasized the company's enthusiasm for IoT in a keynote at its annual developers' forum.

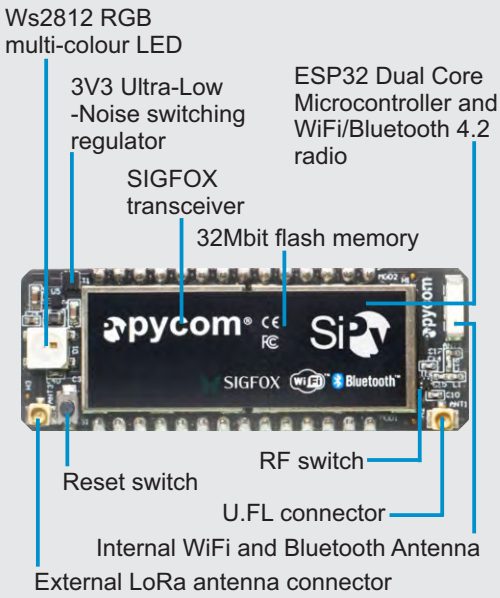
Still, it would seem the practical utility of IoT estimates is limited if they have the potential to be revised by many billions of units. Turner at IDC says such variation and fluidity of these numbers is typical of early estimates focused on nascent markets. The point, he suggests, is to think of the estimates as a general signal, rather than focus on the specific numbers.

There are many reasons why projections from different firms may change over time, or simply not match up in the first place. Each company starts with its own definition of IoT and refines its methods over time.

Pycom Collaborates with Sigfox to bring out The SiPy in October 2016

With Sigfox, WiFi and BLE, the SiPy is the latest Pycom triplebearer MicroPython enabled micro controller on the market today – the perfect enterprise grade IoT platform for your connected Things. With the latest Espressif chipset the SiPy offers a complete combination of power, friendliness and flexibility. Create and connect your things everywhere. Fast.

Size: 55mm x 20mm x 3.5mm



Sigfox Specifiction:
- TI CC1125NarrowbandTransceiver
- Class 0 device. Maxi Tx power:
  - +14dBmEurope
  - +22dBm America
  - +22dBm Australia & New Zealand
- Node range: Up to 50km
- Sigfox pre-certified (Oct.2016)

SiPy Features:
- Powerful CPU, BLE and state of the art WiFi radio
- 1KM Wifi Range
- MicroPython enabled, use Linux IoT for 10x faster programming
- Fits in a standard breadboard
- Ultra-low power usage: a fraction compared to other µ controllers
- 2xUART, 2xSPI, I2C, I2S, µSD card
- Analog channels: 8x12 bit ADCs
- Timers: 4x16 bit with PWM+capture
- DMA on all peripherals
- GPIO: Up to 24

MORE: Click Here
Web Shop: Click Here
Datasheet: Click Here

pycom™

... from Page 7 - IoT Forecast of 50B Devices by 2020 Is Outdated

To begin, many collect annual sales data from manufacturers that produce connected devices, or components such as semiconductors, as well as from companies that sell and ship those products to customers. Then firms subtract a percentage of devices to account for those that will be replaced or thrown out each year. When added to estimates from past years, that leaves the firms with the "install base," or approximate number of connected devices in use at a given time.

Some firms include other variables, such as the amount of money that companies spend annually on information technology. Evans factors in industry growth rates based in part on Moore's Law, the longstanding prediction that the number of transistors in an integrated circuit doubles every year or two, and Metcalfe's Law, which states that the utility of a network increases with each new device that connects to it.

Firms often have no real way to know how many devices that are sold and shipped actually wind up connected to the Internet, so some conduct consumer and business surveys to gauge how devices are used. Morelli at IHS Markit estimates 90 percent of communications devices (including smartphones) are switched on, but perhaps only 50 percent of cars and accessories are ever connected.

Janna Anderson, an expert in emerging technologies at Elon University, says there is a degree of self-interest at play in projections, too. In 2013, she helped the Pew Internet Project survey more than 1,600 experts about what the IoT might look like in 2025. Not surprisingly, she found that "those who are marketing it and those whose bottom line is somehow impacted by enthusiastic predictions are more likely to make them."

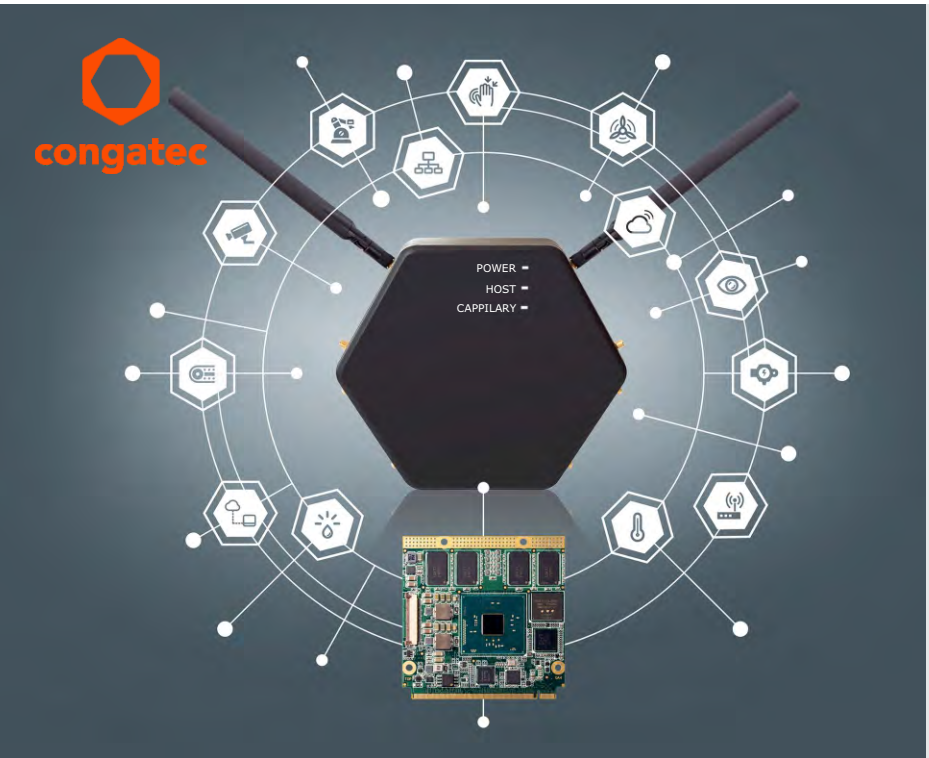
Middleton at Gartner, who publishes one of the most conservative IoT estimates available, also believes boosterism plays a role in some analyses. "It's human nature," he says. "If you're a participant in the industry, and you're launching new products, there's a lot of enthusiasm that builds and a lot of hype."

One of the puzzling things about IoT estimates is that they attempt to anticipate demand for devices that have largely not yet been invented or commercialized. At this point, even the strictest definitions of IoT remain fuzzy because companies are still working on the technologies and business cases. "Will connected pets be a thing of the future? No one knows," Evans says.

In fact, IoT skeptics often point to Bluetooth-enabled toasters as an example of senseless connectivity that will only ever be used by a handful of early adopters. But Evans is confident that entrepreneurs will find many millions of practical ways to serve customers through the IoT in due time. "I think technology needs to solve real problems, and if it doesn't solve real problems in the real world, it's probably a gimmick and will die on the vine," he says.

Though past estimates haven't exactly panned out, Bob Heile, standards director for the Wi-SUN Alliance and chair of IEEE 802.15 (a working group for wireless personal area networks), says the general trend that early IoT analysts predicted has proven true. There are more and more connected devices today than five or 10 years ago, even if they're being connected at a slightly slower rate. "What I do know, because the trend is absolutely undeniable, is more and more things are getting the ability to communicate and connect to something else," he says.

As the next 10 billion IoT devices come online, the industry will face some formidable challenges, such as ensuring the security of its devices, powering billions of sensors, and handling all the resulting e-waste. Despite those issues, Evans isn't bashful about anticipating an even bigger future. "I could see trillions of connected things, ultimately," he says.



congatec introduces highly flexible IoT gateway

Easily customizable for rapid field deployments

The congatec IoT gateway offers extreme levels of flexibility in terms of processing performance and software integration, able to host up to 8 wireless antennas that can be connected to 3 mini PCI Express slots and 6 internal USB based slots for wireless and wired connectivity modules.

OEMs utilizing the conga IoT gateway platformbenefit from a pre-configured, pre-certified IoT gateway that can easily connect a wide range of heterogeneous sensors & systems to cloud-based sevices.

Applications: smart cities, agriculture, connected homes and vehicles, digital signage systems ...
http://www.congatec.com/en.html