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

Jan-Feb 2018

The Need for IoT Advanced Security *Do-It-Yourself Isn't Enough for IoT*

Sensors are Fundamental to New Intelligent Systems

Prices are down to the floor

Microsemi AcuEdge Dev-Kit for Amazon Alexa Voice Service Wins Innovation Award

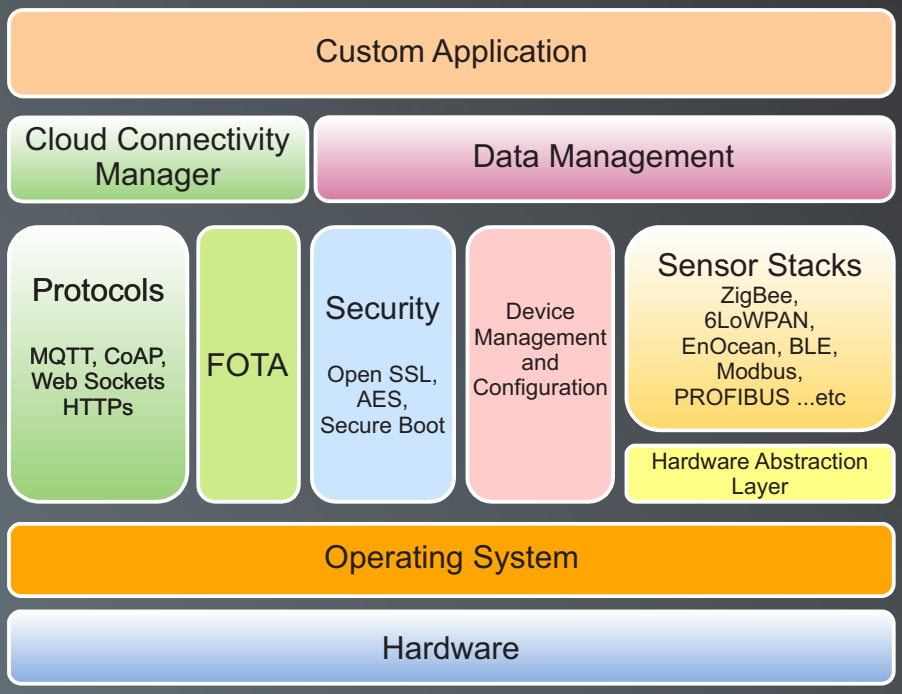
Some 5.5 million New IoT Devices come online EVERY DAY

Gartner: 20+ billion by 2020

75% of people involved in Digital Transformation believe that there is NO Digital Transformation without IoT

What is an IoT Gateway and Why is it so Important for the Success of Projects?

Understanding the Architecture



Adlink New Rugged Compact IoT Gateway Controller

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

In this Edition:

Take also a look at the previous editions click on the logos

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

Over 3 decades Chips & Embedded Systems Market Expertise

Dear Reader,

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

Those e-magazines are distributed Free of charge WORLDWIDE to our PREMIER Database.

Each e-magazines has its own dedicated Website.

Our aim is to provide you with relevant information in relation with your business, we are listening to our READERS in order to adapt the content & the right mix.

In the mean time we have produced and distributed about 2.000 Editions.

FREE Subscription
Click on the logos

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

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

About e2mos SERVICES
See last page:
- Business Development
- Coaching Biz Discovery
- Publications & e-mailings

WHITE PAPER

CENTRI
Advanced Security for IoT

The Need for IoT Advanced Security: Why Do-It-Yourself Isn't Enough for IoT

Introduction: The Critical Need for Effective IoT Security

The Internet of Things (IoT) is growing massively, as is the need for effective IoT security.

Securing the billions of IoT devices already deployed is a top concern – everything from home appliances, to insulin pumps, to implanted pacemakers, to sensors deployed throughout manufacturing, to the spectrum of devices out in the wild controlling the power grid, water supply, and other utilities and services essential to daily life.

The U.S. Department of Homeland Security in a recent report noted: while the benefits of the IoT are undeniable, so too is the reality that security is not keeping up with the pace of innovation.[2]

Some **5.5 million** new IoT devices come online every day — Gartner estimates that by 2020 the IoT will include more than **20 billion** devices.[1]

IoT Security: No Place for Do-it-Yourself « DIY »

IoT security is no place for do-it-yourself (DIY). Even well-seasoned developers – including well-seasoned security developers – should turn to solid third-party expertise when approaching the critically important task of securing an IoT device or network.

"DIY is a bad idea..."
"You have to pick an expert to take on IoT, if you are not one already… there are too many fast-moving pieces, each requiring a certain expertise."[3]

How IoT Security Differs from Traditional Security

The challenge of securing IoT, and the inadequacy of traditional IT security measures, is captured in a recent quote from R. Danes, writing in Silicon Angel:

> *"The idea of a single monolithic firewall to provide protection from cyber threats is becoming a bit quaint. The data center is breaking up and moving to multiple environments – this is true for most companies moving to the cloud and doubly true for those involved in IoT. This is putting demands on these data outposts to do more and raising uncomfortable questions about how they will be secured."*[4]

Why Securing IoT is So Difficult

Securing IoT components – devices, data, and the cloud presents a complex and critically important challenge because they nearly always live beyond the protective firewalls and layers of security found in normal enterprise and mobile computing.

IoT devices can be minimal in size and in what they do, but their functions can be critically important – whether regulating dosage from an insulin pump, to detecting temperature changes in a nuclear power plant. This means that many IoT devices have minimal system resources, and because many are battery operated, it is essential to implement security that has minimum impact on storage, computing, and power needs.

To secure an IoT environment you must provide a complete solution because hackers can now look for and exploit gaps and seams from many more attack surfaces. Completeness includes support for device authentication, encryption for data while in transport, in use on the device and at rest in the cloud, visibility and insight to what is happening across the IoT security environment (including the ability to search your own encrypted data), and a number of other functions such as network bandwidth efficiency, and removing dependence on traditional and unscalable centralized key management for protecting data in use and at rest. Add to this the flexibility needed to work within an unlimited variation of IoT hardware and software architecture, while requiring only a minimal footprint from the standpoint of both storage and computational needs – the demands for a resilient IoT security solution are daunting.

While the above is just a glimpse of what is needed, remember that all of this must be accomplished in a completely secure and integrated fashion.

... to the next page

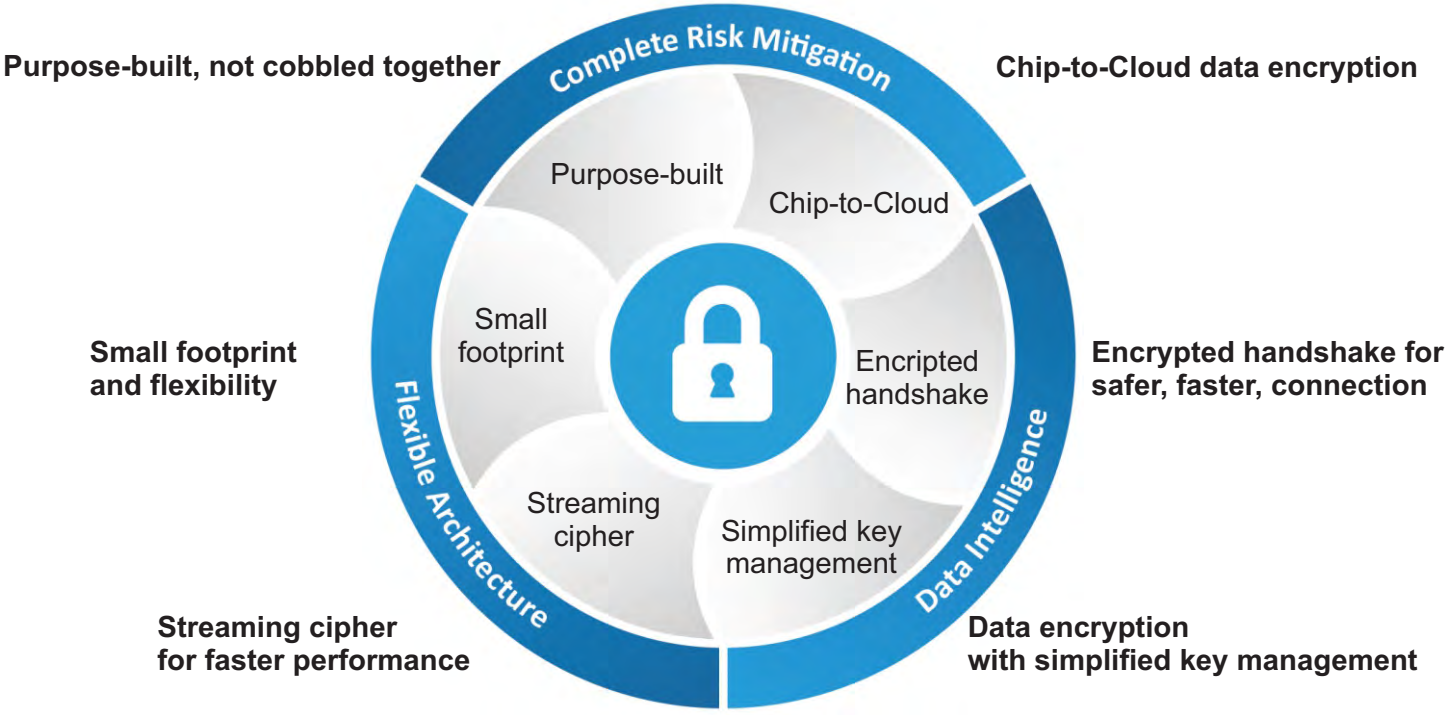
CENTRI
Advanced Security for IoT

The Need for IoT Advanced Security: Why Do-It-Yourself Isn't Enough for IoT

... from previous page

What to Look for in IoT Security

IoT security should be a top priority for product, engineering and security leaders, developers, and all other stakeholders. IoT security should have a flexible design so you can incorporate it into your solution stack, complete security including encryption of data in motion, in use and at rest, and data intelligence to monitor and react to IoT security incidents across your IoT ecosystem.



Securing IoT with CENTRI IoTAS

The CENTRI Internet of Things Advanced Security—IoTAS platform provides a suite of purpose-built, standards-based, advanced security components including leading-edge cipher technology that enables IoT developers to deliver a complete IoT security platform with device integrity, data protection (in motion, in use at the edge, and at rest in the cloud), bandwidth and data storage optimization, IoT device management and insight into all IoT ecosystem data activity.

You can use CENTRI IoTAS to secure your entire IoT ecosystem – from IoT devices, mobile applications, gateways, Cloud infrastructure, and any network connection. Looking at just some of the CENTRI IoTAS components, here's how you can put them to work:

IoTAS
Internet of Things **Advanced Security**

- ✓ CENTRI Secure Communications Endpoint
- ✓ CENTRI Secure Communications Service
- ✓ CENTRI Data Protection
- ✓ CENTRI Secure Manager
- ✓ CENTRI Secure Insights
- ✓ CENTRI Service Layer

Download The White Paper

About CENTRI

CENTRI provides a complete, advanced security solution for the Internet of Things. Our flexible, softwareonly platform enables thing makers and developers to quickly get to market with purpose-built IoT security to protect their data from chip to Cloud. CENTRI eliminates the risk of data theft and delivers device integrity with modern, standards-based technologies for the connected world.

CENTRI HQ | 701 5th Avenue, Suite 550, Seattle WA 98104, USA | +1-206-395-2793 | www.centritechnology.com

ADLINK Launches New Rugged Compact IoT Gateway/Controller

IIoT-ready MXE-210 delivers a secure and robust platform with minimal footprint

Taipei, Taiwan -- 2017/12/01

ADLINK Technology, a global provider of leading edge computing solutions that drive data-to-decision applications across industries, introduces a robust and reliable IIoT-ready combination embedded controller and IoT gateway.

ADLINK's MXE-210 offers a small footprint and is fully operable in harsh environments from -40°C to 85°C, making it an ideal choice for industrial automation, transportation, agriculture/aquaculture, and smart city applications.

Functioning as both a gateway and embedded controller, the MXE-210 bridges the gap between Operations Technology (OT) and Information Technology (IT) data interchanges, with support for third party manufacturers via its wide range of industry standard compliances; **support is included for Modbus, EtherCAT, DDS, MQTT, and CANOpen by Vortex Edge Connect, as well as Wi-Fi, BT, LoRa, 3G, and 4G LTE for data communication and wireless connectivity.** As a controller, the MXE-210 leverages the same protocols to directly communicate with and manage any standard industrial device.

"As Industrial Internet of Things applications continue to expand, manufacturers and other industries require functionality across a range of environments without the need to resource individual manufacturers to meet the conditions of each location." said Ryan Huang, product manager for ADLINK's Embedded Platform & Module Business Unit. "The MXE-210 Series provides **industrial grade EMI/EMS EN 61000-6- 4/2 certified performance in extreme environments and, with EN 50155 EMC compliance, is ideally suited for use with all manner of rolling stock." The MXE-210 gateway's single embedded SIM (e-SIM) automatically switches between regional networks,** enabling a more secure and robust alternative to multiple SIM cards currently to deliver data as rolling stock moves between regions. The pre-installed e-SIM also eliminates time spent swapping out installed SIM cards.

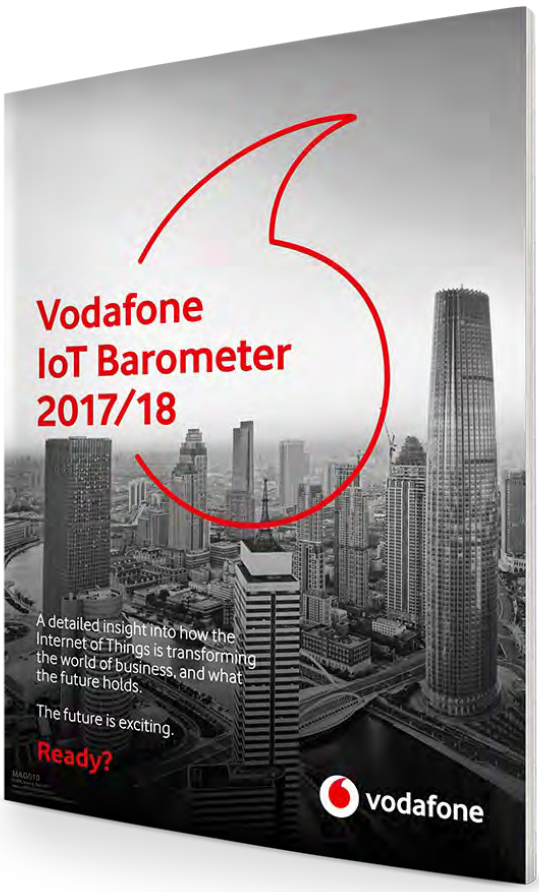
The MXE-210 Series further supports a wide range of comprehensive security measures, providing protection from the inside out with the benefits of TPM 2.0, Intel® Boot Guard, and UEFI Secured Boot. In addition, the MXE-210 comes equipped with an Intel Atom™ x7-E3950/x5-E3930 processor (formally codenamed Apollo Lake-I), one DisplayPort, two USB 2.0, two USB 3.0, two GbE ports, two COM ports(RS232/422/485), two mPCIe slots, one USIM slot, one mSATA, one SATA-III, one Micro SD slot, and support for DIN-rails and wall mounting. Optional extras include audio mic-in, line-out support, eight isolated DI with interrupt and eight isolated DO, and two additional COM ports (RS232/422/485)*.

For more information about our integrated predictive maintenance solution, please visit ADLINK's website HERE.

* Eight isolated DI with interrupt and eight isolated DO, and two additional COM ports (RS232/422/485) will be ready on Q1 2018.

Vodafone IoT Barometer 2017/18

A detailed insight into how the Internet of Things is transforming the world of business, and what the future holds.



Executive summary

1. State of the market
- The proportion of companies using IoT (adopters)
- Organisations using IoT are doing more of it.
- The benefits go way beyond cost-cutting.
- Adopters are getting more sophisticated

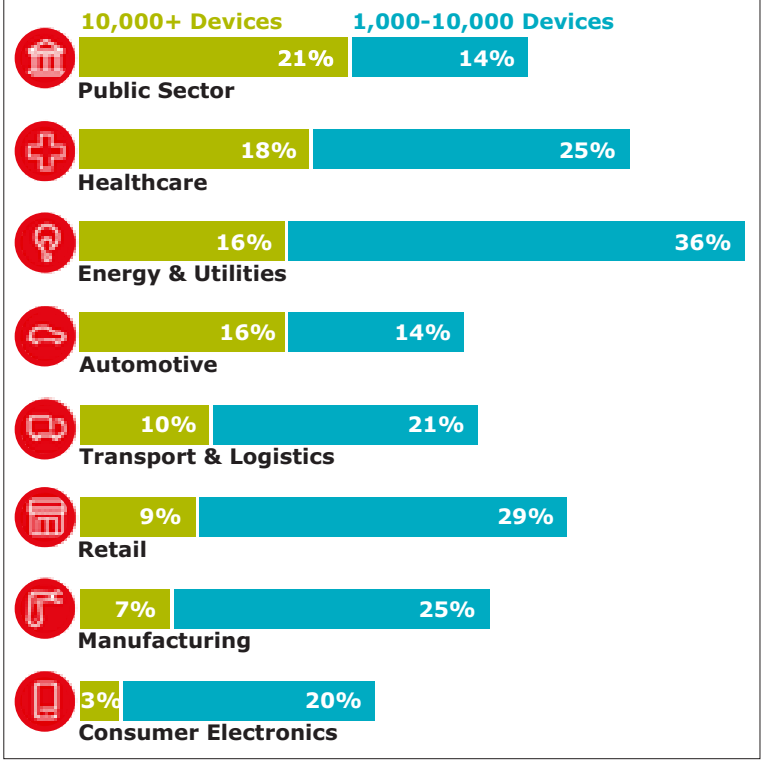
2. The benefits
- Those with the most connected devices are seeing the biggest gains.
- Return on investment can be significant.
- Success is driving increased investment.
- IoT is enabling new and increased revenue.
- IoT is driving business transformation.

3. Moving forward
- Security is still a concern.
- Adopters are looking for partners to fill their skill gaps.
- Adopters want connectivity that's secure, reliable and pervasive.
- New connectivity options could drive the next wave of adoption.

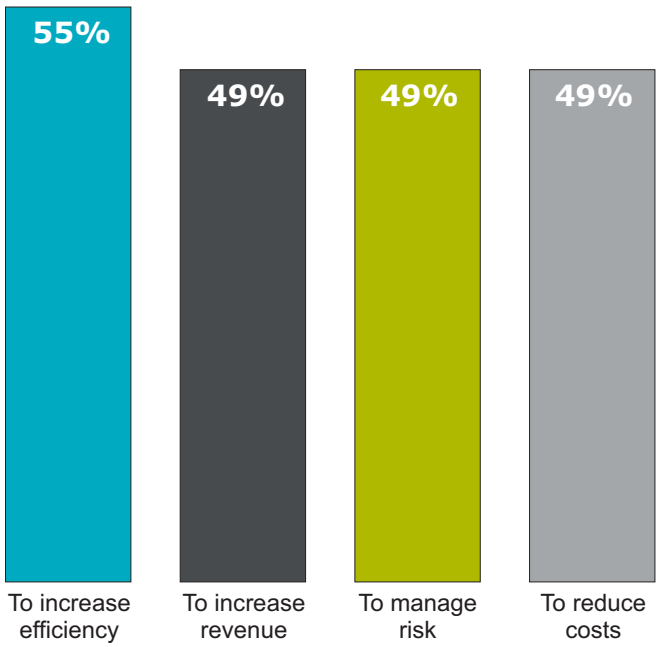
4. The next five years
- Adopters have high expectations.
- IoT will be even more integrated.
- IoT will drive adoption of artificial intelligence (AI).
- Concerns about security will have sened.
- Partnerships will flourish.les

Download your Copy

Number of connected devices



Why adopters are using IoT



Did you know?

Gartner has positioned Vodafone as a "Leader" in its Magic Quadrant for Managed M2M Services, Worldwide report 2017, for the fourth consecutive year

We are the world's largest IoT services provider

Vodafone IoT have connected over 65 million devices worldwide

Microsemi's AcuEdge Development Kit for Amazon Alexa Voice Service Wins "Internet of Things Product Innovation Award" at Elektra European Electronics Industry Awards 2017

ALISO VIEJO, Calif.—Jan. 31, 2018—Microsemi Corporation (Nasdaq: MSCC), a leading provider of semiconductor solutions differentiated by power, security, reliability and performance, today announced its AcuEdge™ Development Kit for Amazon Alexa Voice Service (AVS) won the "Internet of Things (IoT) Product Innovation Award" at the Elektra European Electronics Industry Awards 2017. The prestigious annual award recognizes a semiconductor reference design or system-level product which demonstrates the capabilities and usefulness of the IoT.

Microsemi's AcuEdge Development Kit for Amazon AVS delivers enhanced audio processing to improve voice recognition rates in adverse audio environments for emerging human to machine (H2M) applications in the IoT, industrial IoT and automated assistance markets. The kit enables third-party developers and original design manufacturers (ODMs) to evaluate and incorporate Alexa functionality in H2M applications, while interfacing with Microsemi's Timberwolf™ ZL38063 multi-mic audio processor.

"Microsemi is honored to be recognized with an Elektra Award, as our AcuEdge Development Kit for Amazon AVS leverages our state-of-the-art Timberwolf solution to enable truly innovative H2M applications at a time when this market is experiencing exciting growth," said Roger Holliday, senior vice president and general manager at Microsemi. "Our team prides itself on our ability to tackle the most difficult challenges facing those in the IoT market. As the industry addresses growing demand for reliable, scalable platforms, this device enables developers to quickly and cost-effectively achieve their design criteria."

Judges of the Elektra Awards described Microsemi's AcuEdge Development Kit for Amazon AVS as a "massive leap forward" for developers looking to integrate Alexa functionality into their products. Its features enable voice control and speech recognition both from a distance and in the presence of noise and audio sounds. The kit has a development board that connects directly to a Raspberry Pi and plastic frames to help position microphones and speakers in targeted applications, providing an ease of setup the judges appreciated. As one judge stated, the device is "a clear winner that will help drive development in this fast-growing market."

The Elektra European Electronics Industry Awards showcase the finest new products, technology innovation and company performances of the year for the European electronics industry. Established to celebrate the achievements of individuals and companies across Europe, they present best practices in key areas including, innovation, sales growth and employee motivation. An independent panel of judges assessed the quality of all entries and winners were recognized at a gala dinner at the Grosvenor House Hotel in London in December 2017.

About the AcuEdge Technology and Timberwolf ZL38063 Multi-Mic Audio Processor
Microsemi's AcuEdge's technology consists of license-free, royalty-free audio intellectual property (IP) solutions. It is the compilation of various IPs targeted at processing voice signals in conjunction with noise reduction algorithms, automatic gain control, echo cancellation, psychoacoustic noise reduction, howling detection and rejection. These powerful capabilities are the foundation for enterprise level automatic speech recognition, sound classification and other intelligent decision-making functions based on sound and audio detection. The ZL38063 Timberwolf provides a powerful digital signal processor (DSP) with voice specific hardware accelerators, three digital microphone interfaces, two independent 16-bit digital-to-analog converters (DACs) with headphone drivers and two flexible time-division multiplexed (TDM) interfaces in a single 64-pin QFN package. Additional features include 44.1/48 kHz stereo music playback with voice, ultralow and standby off power, and stationary and psychoacoustic noise reduction. It can run unattended (controllerless) and offers self-booting into a configured operational state. In addition, the ZL38063 has built-in support for G.712 and G.722 and is G.168 and G.169 compliant line echo cancellation (LEC). To learn more about the ZL38063 visit https://www.microsemi.com/products/audio-processing/home-automation/zl38063.
For more information about the Development Kit for Amazon AVS visit:
https://www.microsemi.com/product-directory/connected-home/4628-zlk38avs.

About Microsemi
Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions, security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, California, and has approximately 4,800 employees globally. Learn more at www.microsemi.com.

Microsemi

amazon

PICMG Overview of IIoT Initiatives

February 15, 2018 by: Doug Sandy, VP Technology PICMG

At PICMG, we have kicked off a new focus on the requirements for Industrial IoT (IIoT). From there, our efforts can expand out to other IoT market requirements. In IIoT, hardware and software interoperability tends to be more important than household/consumer applications as sensors, actuators, and controllers from multiple vendors must work together seamlessly. But, standardization has not yet materialized.

IIoT, is different than traditional industrial automation in the fact that it combines ubiquitous sensing, advanced analytics, and IT technology. Going beyond traditional automation control functions, IIoT includes sensors and actuators for facility operations, machine health, ambient conditions, quality, and a variety of other functions. Advanced analytics enables the IIoT system to realize higher levels of operational efficiency by extracting meaning from the potential data available from a vast array of deployed sensors. Similar to cloud data centers, where sensors data is used to optimize virtually every aspect of operational efficiency, smart factories and other IIoT applications utilize analytics to improve up-time, optimize asset utilization, and reduce overhead costs. Migration to IT technology enables the IIoT operator(s) to deploy, monitor, and optimize their IIoT application. Standardization around IT practices helps to eliminate islands of proprietary equipment within the installation and provide tighter integration between the control domain and the operations domain. Adoption of IT methodologies enables IIoT companies to leverage the large existing base of IT hardware and software solutions when appropriate. Each of these benefits offers significant potential for capital and operational savings.

Standardization of the upstream interfaces for controller devices and meta-data models for sensors can help solve hardware and software interoperability and ease-of-use issues. Standardized interfaces would allow dissimilar pieces of hardware to communicate with the IIoT command center in a uniform fashion and eliminate isolated islands within the installment. Likewise, an extensible standardized meta-data model for sensors would allow for systematic detection and control of sensors and control points without extensive code re-writes. From a hardware standpoint, the IIoT marketplace would also benefit from greater standardization around communications interfaces, power, and environmental requirements.

Large industrial automation suppliers are not incentivized to embark on open standardization because it loosens the customer's dependence upon their proprietary solutions. Smaller automation suppliers lack the industry clout or size to take on such an ambitious undertaking. This is a task best suited for an industry standards organization, and one which PICMG is well equipped to handle.

COM Express is one logical starting point to build upon because it has the small form factor, processing performance, and flexible I/O configuration to make it a natural fit for small gateways and control functions in small to medium installations, with distributed controllers for larger deployments. In larger installations, CompactPCI Serial or MicroTCA have been adapted for railway control and other rugged applications and may also serve as a flexible gateway/controller. Click on the full IIoT Overview Discussion for more details.

PICMG open-standards embedded computing organization sets sights on postage stamp-sized computer board

January 23, 2018 by MIL & AERO

A new generation of small-form-factor embedded computing may be coming together at the PICMG Open Modular Computing Standards organization in Wakefield, Mass. -- a computer board no larger than a postage stamp for wearable computing, smart factories, and the Internet of Things (IoT).

This project, just in its infancy, sees to develop an industry-backed open-systems standard for a tiny embedded computer with minimal processing and minimal I/O resources for lightweight applications that must operate in extremely tight spaces.

PICMG, formerly known as the PCI Industrial Computer Manufacturers Group, is likely to stand-up a Postage Stamp standards working group sometime this spring, and may have its first draft standard ready for balloting by 2019, says PICMG President Jessica Isquith.

Postage Stamp likely will describe extremely small embedded computing mezzanine cards ranging in size from a postage stamp to a business card for operating close to assets on a factory floor and similar applications. Isquith made her comments this week at the Embedded Tech Trends conference in Austin, Texas.

This potential future standard probably won't be for anything like high-performance embedded computing -- only for extreme size- and weight-sensitive applications operating near antennas and sensors, in robotic arms, in data analytics uses, and the like It may operate together on a carrier card for handling several separate tasks.

It's far too early to speculate on specific characteristics for the Postage Stamp embedded computing form factor. PICMG members have shown interest, and developments later this year will be the first indications of the directions this standard will take.

Anyone in the embedded computing industry interested in influencing and working with the future Postage Stamp standard should contact Isquith by email at jess@picmg.org.

OPTION WIRELESS TECHNOLOGY

Bring the Internet of Things to your business with CloudGate, smart wireless IoT solutions

Includes LTE, 3G, Ethernet, GPS and customizable modules compatibility
Learn more about hardware

Connects through WiFi, Ethernet, USB, RS232, RS485, Digital I/O, Analog I/O, etc

Connect virtually anything to our CloudGate Gateway

Connectivity and on-board processing power
Easy-to-install. Powerful. Carrier-approved.

Custom tailor each device to your own specifications and provision your hardware from anywhere

Reliable. Secure. Flexible, with open source SDK. User friendly, thanks to 'visual wiring'.
Learn more about CloudGate Universe and Luvit-RED Click HEre

Take control of your environment and start saving now

Cost-effective integration. Free quote.

LuvitRED LoRa SRAS
SECURE REMOTE ACCESS SERVICE

Option Engineering Services

Option backs its advanced CloudGate M2M solution platform with an extensive engineering consultancy capable of helping you succeed. Our talent and experience have proven extremely effective in helping companies effectively and efficiently develop products.

We work with organizations which seek to leverage our years of specialized wireless communications experience to speed time-to-market, reduce risk and proactively avoid product design and development pitfalls.

Option's Engineering Services and our in-house and state-of-the-art OptionLab, are here to help you recognize and capitalize on market opportunities. From early stage product feasibility assessments, to final product manufacturing, our Engineering Services can support your full range of needs.
For more information, consult www.engineering.option.com

Download the brochure

Contact us







Adlink
IoT Solutions and Technology
(Formerly PrismTech)

Transportation

Vortex DDS provides a unique ability to address the real-time data distribution requirements of large scale, complex transport management and connected vehicle systems.

The Internet of Things (IoT) is revolutionizing transportation by helping to deliver smarter, connected vehicles and transportation systems that are safer, more reliable, greener, cheaper and provide an improved passenger experience.

Transportation falls into three main segments all of which can benefit from the connectivity offered delivered by the Internet of Things:

- **Vehicles -** this includes vehicle telematics, tracking and mobile communications with cars, trucks and trailers. Vehicle telematics then enables services like navigation, vehicle diagnostics and supply chain integration. Other vehicle-related areas include off-highway (e.g. agricultural and construction).
- **Non-Vehicular -** this includes aircraft, trains, ships/boats and containers.
- **Transport Systems -** this includes passenger information services, road pricing schemes, parking schemes and congestion charging, particularly in cities.

A common characteristic of transportation is that it needs to be able to cope with increasingly high volumes of data. It also has a strong requirement for scalable, performant real-time data delivery with extensive Quality of Service (QoS) properties.

The Vortex DDS product suite is an ideal solution to meet the transportation connectivity requirements of the IoT. Vortex uses as its underlying technology the Data Distribution Service for Real-Time Systems (DDS) standard and delivers a proven real-time data delivery and connectivity solution with extensive (over twenty) QoS. Vortex DDS enables real-time coordination of telemetry data with other sensor data to optimize complex rail, trucking and fleet operations. Vortex DDS is able to connect from the smallest edge device such as a parking sensor to the largest system of systems such as air traffic control and is able to deliver the right data to the right place at the right time all the time. With rich information, Vortex customers are able to deliver more goods and people on time at a lower cost: improving the quality of service and reducing supply chain costs.

Featured Clients

Coflight

Coflight Consortium Selects Vortex OpenSplice DDS Middleware for Next Generation European Flight Data Processor.

The Coflight Consortium headed by THALES and SELEX-SI has selected our OMG Data Distribution Service...

ProRail

ProRail Deploys Vortex OpenSplice for Dutch Railway Network.

Vortex OpenSplice provides ProRail with a reliable, real-time and fault-tolerant data-sharing platform to manage critical information within the railway system....

PR: Coflight Published on 21-Feb-2018 by Ministère de la Transition écologique et solidaire

COFLIGHT One of the most advanced Flight Data Processing Systems (FDPS) in Europe

COFLIGHT deliveries a remote Flight Data Processing service to ANSPs. It enhances European ATM Performance

Coflight, is one of the most advanced Flight Data Processing Systems (FDPS) in Europe, designed and developped by a Franco-Italian coopération (DSNA-ENAV & Thales-Selex ES) on e-FDP Eurocontrol specifications. Coflight is compliant with all new European standards.

With « Coflight as a Service », DSNA and ENAV will provide FDP remote service and system maintenance to ANSPs. It will be made avaible to the customers via a SWIM compliant, cloud computing system.

What is an IoT Gateway Device and Why is it so Important for the Success of IoT Projects?

By Embitel https://www.embitel.com/
Embitel is now a company of Magento Enterprise Solution Partner in UAE & Kuwait

IHS forecast suggests that the growth in number of IoT devices will be exponential, with an installed base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025.

Now to support such network(s) of IoT devices that are expected to become more complex, IoT Gateway is one of the most critical components of the entire Internet of Things (IoT) network.

Image Source: Intel

What is an IoT Gateway Device?

IoT Gateway, as a hardware device or a virtual software code, acts as a communication bridge between IoT Sensor Network and Cloud Server.

IoT gateway device has a layered architecture. Following are some of the important software and hardware layers to help you get better understanding regarding the IoT Gateway Development process:

1.) Hardware Platform: This defines the processing power & memory specifications of the IoT Gateway. This is the gateway powerhouse and a hardware platform is selected based on the complexity of IoT application(s) that need to be deployed

2) Operating System: The decision of opting for a particular OS depends on the legacy systems. It is a best practice to continue to use the OS compatible with the existing systems in order to save costs and hassle-free integration

3.) Analytics Engine: This layer ensures raw data is converted to actionable insights

4.) Integrated Application development platform and Device Drivers: This layer supports development and/or addition of new devices, applications or systems to the IoT network

Why IoT Gateway is important?

The importance of an IoT Gateway device can be gauged by the number of critical tasks/actions that are performed by this device.

Here is just a glimpse of some of the important tasks:
Facilitate compatibility across the IoT network. IoT Gateway ensures this by supporting a number of communication protocols like Zigbee, 6lowpan, Bluetooth, WiFi, LoRA, Zwave
All the devices that need to be monitored or controlled have relevant sensors installed on them (temperature, humidity, proximity or other sensors).

These sensors are IP based; IoT Gateway manages the connectivity of these sensors (and in turn real world physical devices) to the cloud server.

To be precise, IoT Gateway makes the devices available online through sensors and cloud
In additional to bringing the IoT network to life, IoT Gateway also performs many operational tasks – manage device configuration, perform device authentication for secure network access and support edge-analytics

... to next page

What is an IoT Gateway Device and Why is it so Important for the Success of IoT Projects?

... from previous page

By Embitel https://www.embitel.com/
Embitel is now a company of Magento Enterprise Solution Partner in UAE & Kuwait

Evolution of IoT Gateway and Edge Analytics

1st Generation IoT Gateway:
These IoT Gateway devices were designed to facilitate communication protocol compatibility and device management functions. However, they did not support data analytics at the 'edge'. With 1st generation IoT Gateway, all the analytics is performed at the cloud server.

2nd Generation IoT Gateway:
This product line of "smart" IoT gateways support 'edge analytics' , hence ensuring reduction in data transfer costs and extension of the benefits of data analytics at local networks

3rd Generation (Current):
This new generation of IoT gateway devices improves the overall system responsiveness and also supports new operating models. Since IoT gateway devices continuously receive huge amount of data from the sensors, at times it may overload the main system. To avoid this the new generation IoT gateway analyzes the data received from various sensors and prioritizes and passes critical information to the main system and send alerts if required.

The new generation IoT gateways are intelligent and capable of filtering out the high priority information from the data received. They are also capable of taking action on the data received. For example, if the gateway senses that the temperature is too high, the gateway can send instructions to turn on the air conditioner.

In our next blog post we will discuss about "How an IoT gateway works". Subscribe to our blog to get alerts about happenings around IoT.

Learn more about our IoT development Services for home automation and Industrial Automation.

How an IoT Gateway Device Works: Understanding the Architecture

By Embitel https://www.embitel.com/
Embitel is now a company of Magento Enterprise Solution Partner in UAE & Kuwait

In our quest to understand IoT Gateway devices better, we requested our IoT Software Developers to shed some light on the technology architecture of the IoT Gateway.

Following are the excerpts from this conversation. If you are an IoT software or hardware developer or an IoT enthusiast, this blog can serve as a good starting point for understanding the various software/hardware modules of the IoT Gateway

Understanding IoT Gateway Architecture – an overview

Design of an IoT Gateway is driven by the 'Custom Application' [e.g – fleet management, asset tracking, industrial automation, connected car, infotainment & more]

As an IoT developer, based on the requirement of the application one needs to calibrate the following:

- IoT Sensors range
- Power demands
- Performance
- Scalability and security

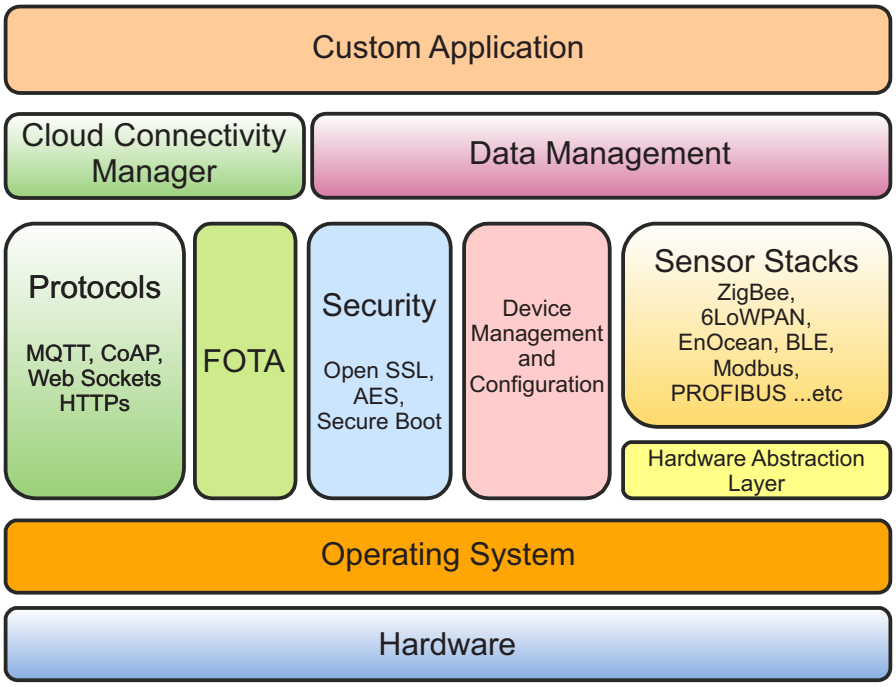
In reference to the below IoT gateway architecture diagram, let us try to understand the various modules or building blocks of the IoT Gateway Device.

... to next page

How an IoT Gateway Device Works: Understanding the Architecture

... from previous page

By Embitel https://www.embitel.com/
Embitel is now a company of Magento Enterprise Solution Partner in UAE & Kuwait



IoT Gateway Device Hardware

IoT Gateway Hardware comprises of processor/microcontroller, IoT sensors, protection circuitry, connectivity modules (e.g Zigbee, Bluetooth, WiFi and more).

Type of hardware (processor/microcontroller), processing speed and memory space is decided based on the Operating System of the IoT Gateway device.

The end-user application also has a big say in the design of the IoT Hardware.

A small to a medium scale application can run on a microcontroller; however if the gateway is expected to do complex operations a processor is needed.

This will have a direct impact on the cost of the gateway device.

As an IoT Development partner or vendor, one should always design hardware components by considering performance, cost and efficiency.

Operating System

Selection of the Operating system is also largely dependent on the IoT application.

If the gateway is to be designed for a simple to medium scale application then a RTOS (Real Time Operating System) is used; however if the gateway has to perform considerably complex operations then Linux is preferred

For the applications like Car HUD or Infotainment systems that require rich GUI then Android OS is the preferred choice.

HAL (Hardware Abstraction Layer)

Hardware Abstraction Layer supports reusability and portability of the IoT software.

This layer makes the software design independent of the underlying hardware platform. Hence it helps to reduce the time and cost required to port the developed software application into a different hardware platform (during migration from the existing platform or re-design of the product line).

... to next page

How an IoT Gateway Device Works: Understanding the Architecture

... from previous page

By Embitel https://www.embitel.com/
Embitel is now a company of Magento Enterprise Solution Partner in UAE & Kuwait

IoT Sensors Stack

This layer basically consists of software stacks that serve as interfaces with IoT sensors modules.

Specific stack(s) is/are integrated depending on the sensor interface the IoT Gateway has to support. Some of the populary integrated stacks are ZigBee, 6LoWPAN, EnOcean, BLE, Modbus, PROFIBUS and more.

Device Management and Configuration

An IoT gateway needs to interface with different types of Sensor devices and each sensor node (used for capturing distinct data) has different set of properties.

IoT Gateway device is required to keep track of all the connected devices/sensors.

In addition to this, all the devices/sensors management and configuration tasks are performed at the IoT Gateway.

Thus it is important that the IoT Gateway Device is easily configurable to manage IoT Sensor settings, properties and access control.

The configuration and settings of all the IoT Sensor Devices is stored in the gateway device memory. This ensures that the last saved settings are available after every re-boot.

Security

Gateway security is one of the key considerations in IoT gateway architecture during the IoT Gateway design process.

The designed IoT gateway should ensure robust data security, device security and network security.

Device security and device identity is implemented in the gateway hardware using Crypto Authentication chips. To add further security to the IoT gateway hardware tampering is implemented.

Secure boot is also implemented to ensure that the gateway doesn't boot from an unauthorized firmware.

All messages between gateway and cloud, and messages between Gateway sensor node is encrypted to ensure data integrity, and confidentiality of sensor nodes. Data to and from every node in a IoT application is encrypted to ensure network security.

FOTA

Ensuring IoT Gateway security requires continuous and timely efforts; as an IoT Development Partner, one needs to keep fixing the security loop holes fixed and maintain device integrity.

Firmware Over The Air (FOTA) updates makes this possible! FOTA updates ensure that the IoT Gateway software is updated with latest versions of security patches, OS, Firewalls and more.

Within the IoT network, the gateway device periodically checks for firmware updates in the cloud and fetches the update.

In case of failure IoT Gateway reverts to the last best known state. Before the update process begins, IoT Gateway checks if the available firmware version is from a trusted source.

Data Communication Protocols

The IoT Gateway connects with the Cloud over Ethernet, Wi-Fi or a 4G/3G modem. Two way communication channel is established with the Cloud for data exchange and command(s) transfer.

The underlying communication layer is UDP or TCP IP protocol.

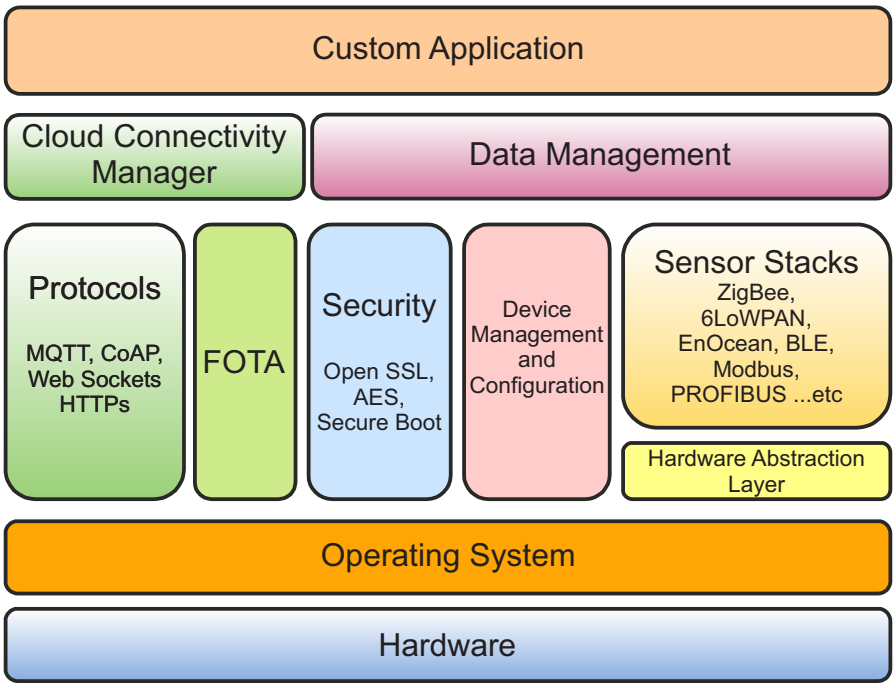
For ease of development and to maintain standardization, protocols like MQTT, CoAP, XMPP, AMQP are utilised. This is because handling and maintaining communication with cloud over raw socket is more complex process.
Protocol(s) is/are selected considering the amount and frequency of the data that has to be shared with the Cloud.

... to next page

How an IoT Gateway Device Works: Understanding the Architecture

... from previous page

By Embitel https://www.embitel.com/
Embitel is now a company of Magento Enterprise Solution Partner in UAE & Kuwait



Data Management

Data Management includes data streaming, data filtering & data storing; in case of loss of connectivity with the cloud.

IoT Gateway manages the data from sensor nodes to gateway and also the data from gateway to cloud.

The challenge here is to minimize the delay to ensure data fidelity.

Cloud Connectivity Manager

This layer is responsible for seamless connectivity with the cloud and also handles scenarios like reconnection, device state, heartbeat message, and gateway device authentication with the cloud.

Custom Application

IoT Gateway application is custom designed as per the business needs.

Gateway application interacts with services and functions from all the other layers or modules to manage data between sensor node and gateway and from gateway to cloud in an efficient, secure and responsive manner.

Gateway Data Transfer

IoT gateway can be connected to the internet for data transfer using Ethernet, 4G/3G/GPRS modem or Wifi. Non-GPRS network is the most preferred mode of internet connectivity. This is due to the cost effectiveness of the data transfer through Wifi or Ethernet.

The gateway should have in-built intelligence to analyze and decide which data should be transferred over the network for processing and which data can be cached for offline processing to save the data transfer cost and processing power of the main application.

After understanding the architecture, one realizes that the Design and development of an IoT Gateway device is a work of art!

As an IoT SW & HW developer, it is very important to understand the business needs (and logic) of the IoT App.

This understanding of the IoT Application is an important factor that contributes to the development of a win-win IoT Gateway design

Though some very popular off-the shelf IoT Gateway solutions are available, but certain customization becomes a necessity to transform a product concept into business reality!

Sensors are Fundamental to New Intelligent Systems

By: GREG LEBSACK, GENERAL MANAGER, MENTOR, A SIEMENS BUSINESS

The evolution of the basic sensors to intelligent electronic sensors is creating a revolution in how we gather useful data from the world around us, analyze that data to make decisions, and connect together vast intelligence systems to enable new solutions and to accomplish tasks that we have never been able to perform before. This opens up the market to new ideas for existing companies and start-ups. Suddenly, sensor-based product development is exciting again and we see design teams tackling new challenges from IoT to Industrial IoT in order to deliver new solutions.

It is believed that first intelligent electronic sensor was proposed in 1980 (by S. Middelhoek and J.B. Angell). It consisted of a MEMS sensor, analog-to-digital (A to D) converter, with the new idea to connect to a processor. However, MEMs and CMOS processor technology was not ready at that time to create this integrated device. But now, the technology is available and it is clear today that intelligent sensors are the key for the development for innovative IoT systems.

Most would agree that the intelligent sensor must contain these key elements (Figure 1):
A sensing device that measures physical parameters from the real world.
A computational block, such as a processor or DSP, that analyzes the sensing device measurements.
A communication block, such as a wireless transmitter, that exchanges information with the bigger intelligent system.

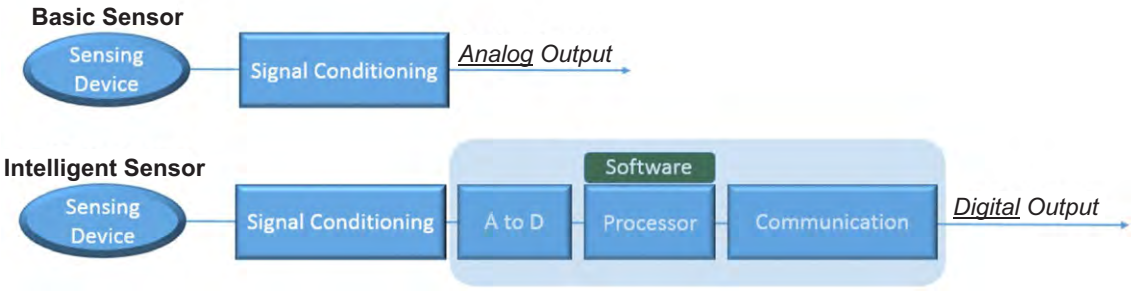


Figure 1: Comparing basic and intelligent sensors.

In addition, signal conditioning is required to transform the sensing device signal into data that the intelligent sensor can use. This conditioning can include amplification, or signal clean up or tuning. The A to D block converts the analog sensing signal to digital so that the processor and software can utilize the information and perform sensor calibration.

THE SENSOR MARKET

Designers can create electronic sensors using a variety of technologies including silicon photonics, CMOS, fluidic chips, and LEDs. But, MEMS sensors are the most interesting technology to explore due to their wide footprint in the intelligent sensor market. According to the Yole Développement's "Status of the MEMS Industry 2017" report, the MEMS sensor market in 2016 exceeded $11 billion in sales (Figure 2).

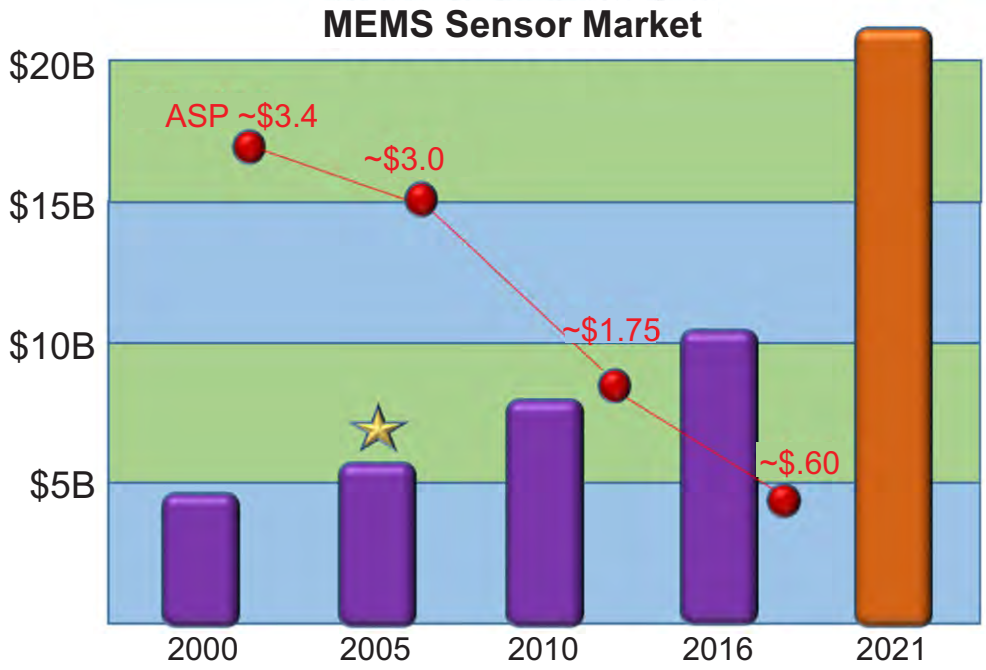


Figure 2: The MEMS sensor market with falling ASP.

... to next page

Sensors are Fundamental to New Intelligent Systems

By: GREG LEBSACK, GENERAL MANAGER, MENTOR, A SIEMENS BUSINESS

... from previous page

In 2003, Knowles Corporation® created the first MEMS microphone and due to its form-factor and resistance to heat that allows surface mounting, the product found its way into smartphones. Then in 2005, smartphones with accelerometers came into the market and accelerated the current MEMs sensor growth. In 2016, there was a big increase in the use of RF MEMS filters due to the complexities of 4G/5G communication, according to the Yole Développement report. But, the average selling price (ASP) of sensors has fallen to about $1 (more on that later). RF and microphones top the units shipped2 followed by the top five MEMS sensors by type (Figure 3).

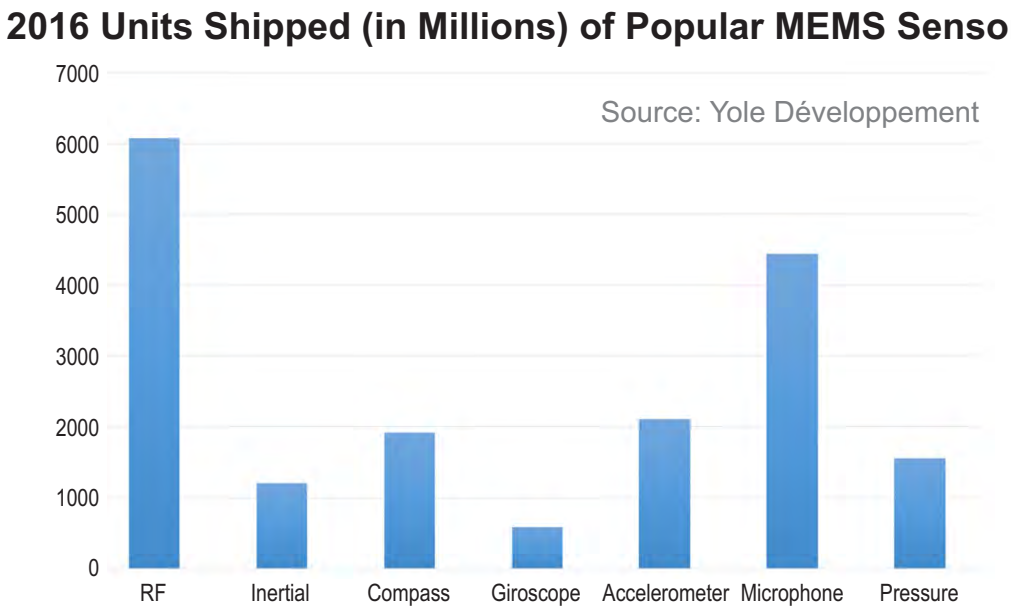
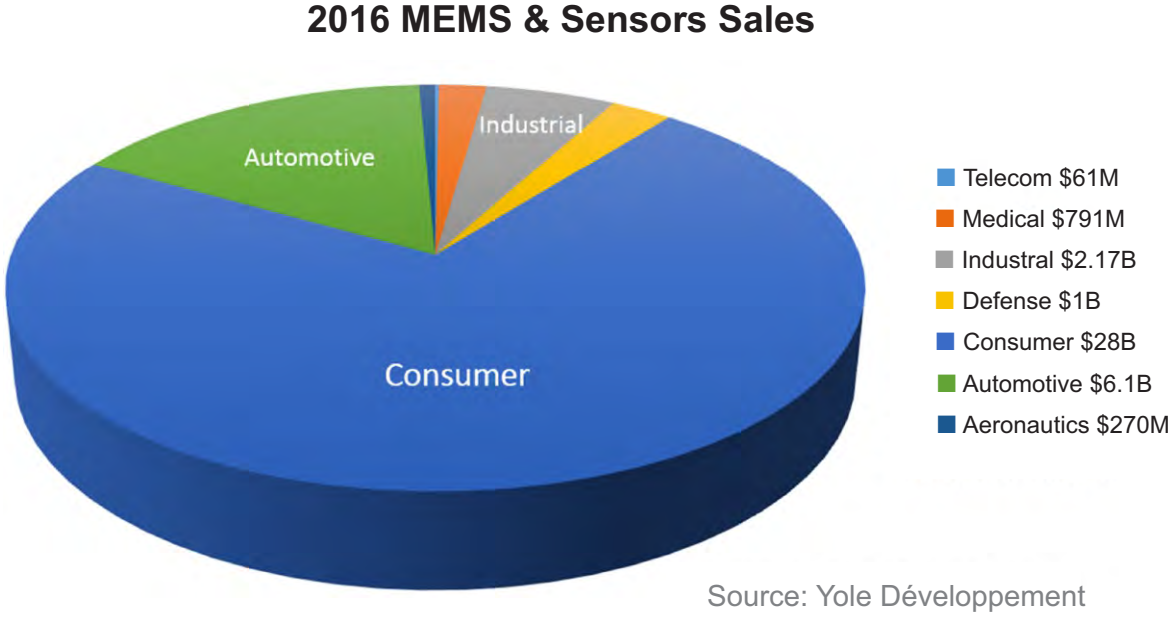


Figure 3: The most popular MEMS sensors sold by type.

If we examine overall MEMS and sensor sales, the consumer market, which includes smartphones, drones, smart home devices, and wearables, is by far the biggest market for combined MEMS and sensors. The automotive market comes in second with driver assistance, safety, and self-driving technology that are laden with sensors. The industrial market is driving sensor purchases for the Industrial IoT (Figure 4).



... to next page

Sensors are Fundamental to New Intelligent Systems

By: GREG LEBSACK, GENERAL MANAGER, MENTOR, A SIEMENS BUSINESS

... from previous page

SHOW ME THE MONEY

Given that the ASP of MEMS sensors is approximately 60 cents a unit, how will vendors make money in the IoT marketplace? If you are a market leader and you ship billions of sensors, then volume is a revenue factor. Or mergers and acquisitions can broaden the market. However, there are other approaches that vendors are taking to bring in revenue. One approach is sensor fusion.

Sensor fusion means developing a product that combines multiple sensors and intelligent software to create a high-value system that is more accurate than using the individual sensors. A good example is the InvenSense (TDK®) ICM-20728, the world's first integrated 7-axis MotionTracking™ device (Figure 5). This device contains a 3-axis gyroscope, 3-axis accelerometer, and a pressure sensor in a single-chip platform solution with an onboard digital motion processor and firmware algorithms.

Figure 5: The TDK sensor system on a chip (Source: TDK).

Software opens the gate to new revenue paths. For example, vendors can offer a portfolio of application-specific products at different price points where the hardware remains the same, but the intelligent sensor functionality is solely controlled by the software. Because the sensor is connected to other sensors and the Internet, the vendor can move into services. These services can include data fusion to optimize systems or to calibrate sensor systems remotely, providing data analysis, or performing remote diagnostics and maintenance.

TANNER LEADS THE WAY

From hobbyists, to small and large companies, designers are taking their new IoT ideas to market by taking advantage of intelligent sensors. A new breed of designers has arrived and they are making hardware design trendy again.

This new breed of designers are reshaping design flows and they have new expectations. They typically work in small teams and require integrated design flows to quickly and easily produce a functioning device while spending as little money as possible. They require the capability to develop a proof-of-concept for system validation in order to capitalize on the opportunity of the IoT market. Design teams need to rapidly implement products using integrated design flows that allow them to quickly develop all the pieces needed for the sensor-driven IoT edge device, including: sensing elements, analog circuit interfaces, analog-to-digital logic, digital logic, and RF, all at a low cost compared to traditional IC and systems design.

... to next page

Sensors are Fundamental to New Intelligent Systems

By: GREG LEBSACK, GENERAL MANAGER, MENTOR, A SIEMENS BUSINESS

... from previous page

Many design teams employ the integrated IC design and verification solution from Tanner to create intelligent sensor-based IoT systems, including Knowles (see the case study here) and InvenSense (TDK). Why? Creating a sensor-based IoT edge device (Figure 6) is challenging, due to the multiple design domains involved.

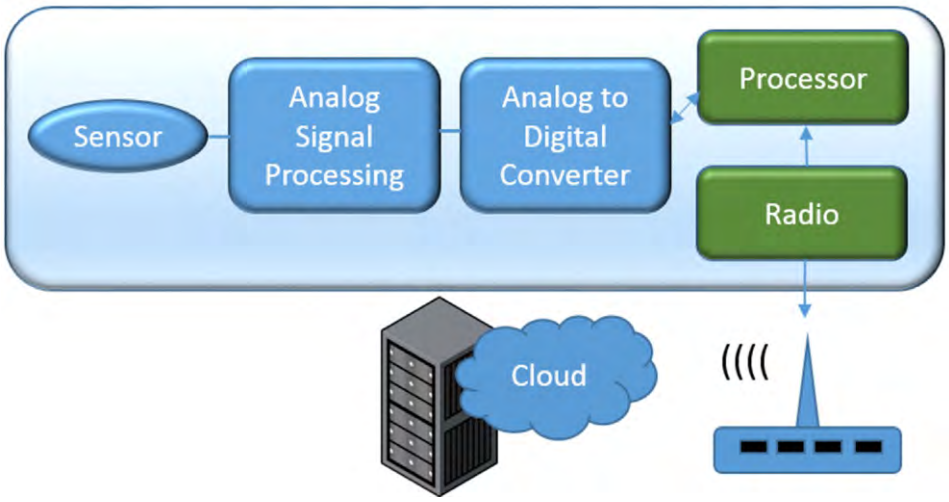


Figure 6: A typical IoT edge device showing multiple domain design.

But, creating an edge device that combines the electronics using the traditional CMOS IC flow and MEMS sensors on the same silicon die can seem impossible. In fact, many IoT edge devices combine multiple dies in a single package, separating electronics from the MEMS design. The Tanner AMS IC design flow accommodates single or multiple die techniques for successful IoT edge device design and verification.

Tanner provides a single, top-down design flow (Figure 7) for IoT design, unifying the analog, digital, RF, and MEMS design domains. Whether you are designing a single die or multiple die IoT device, you can use the Tanner design flow for design, simulation, layout and verification.

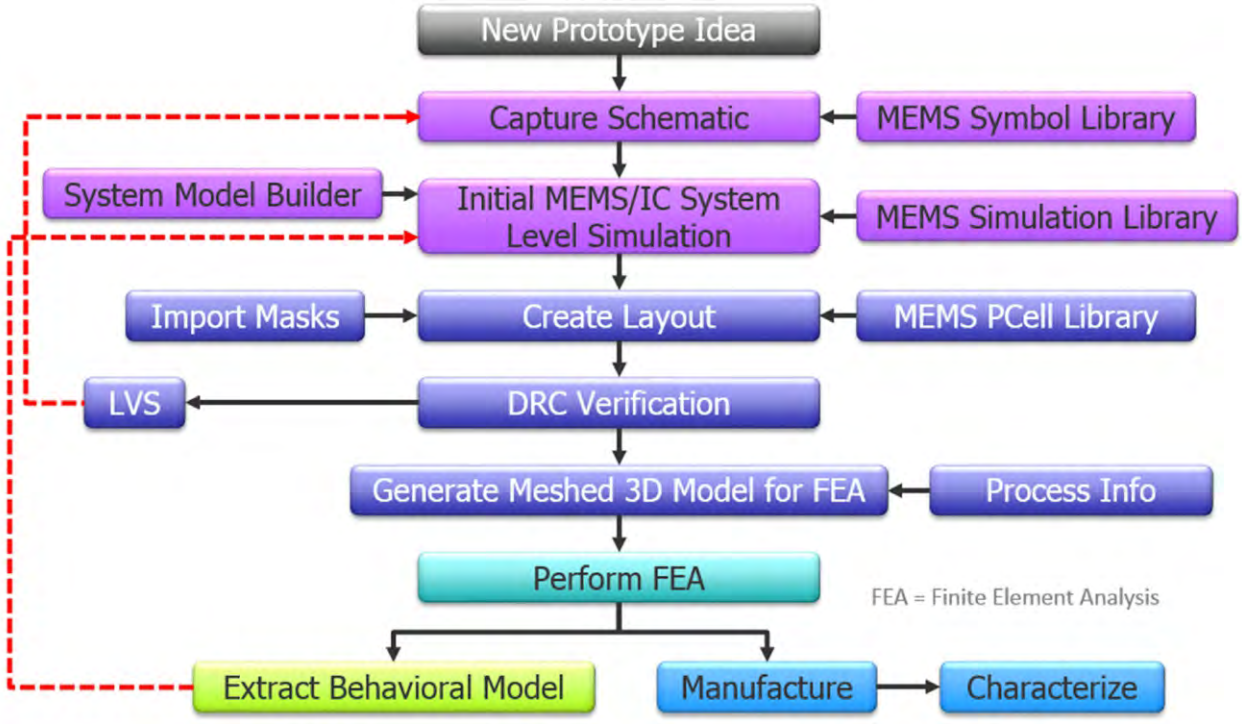


Figure 7: A single top-down design flow for multi-domain design and verification.

Mentor recognized early the opportunities that the IoT edge opens up to the new breed of designers and offers them a unique solution, tailored to their requirements.

To learn more about the Tanner solution for intelligent IoT systems, view the website here. To read about how Knowles Corporation used the Tanner flow to create their MEMS micro

For the latest product information, please visit: www.mentor.com

Office locations and Worldwide Distributors, including all phone numbers please CLICK HERE

Mentor®
A Siemens Business

Time to adapt your Business Discovery Strategy

We connect Suppliers with More Customers ...Much Faster

GLOBAL REFERENCES include: IBM, Intel, Microsoft, Cisco/Tail-f Systems, Telco Systems, Artesyn, Motorola, TI DSP, Xilinx, Adlink, Kontron, Radisys, Enea Software, Green Hills Software, Wintegra, Arrow, Avnet, … and more

Our SERVICES for HW & SW Vendors addressing OEMs and Service Providers

Meet New Customers

Customer Meetings Setup for New Business with the RIGHT Decision Makers

We provide Excellent Results based-on Deep Customer Relationship and Product/Market Expertise
OPTION: we join the Customer Meeting

Make a Big Jump Take a Tiger for a while

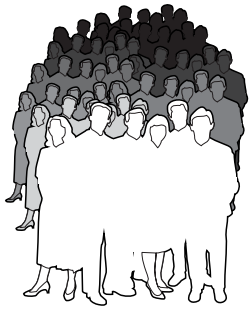
Coaching
How to find More New Customers Strategy Setup Hands-on

Audit: what are you doing today
Targets: what do you want
Our recommendations
How to get there

We bring you to the Frontline

Market Presence Acceleration
Massive Global Reach
Five e-magazines with High Focus

The KEY-to-SUCCESS of our Magazines is the Quality of our PREMIER Database and the ongoing UPDATING done Every Day by RESEARCH from many sources



Click on the logo's

aiworld

Market Focus: related to Artificial Intelligence from A to Z
Major Players

IoT World

Market Focus: related to Internet of Things
IoT HW & SW - M2M
MEMS - Sensors
Solutions
Service Providers

Embedded Systems World

OEM Focus: Automation, Energy, Transportation, Medical, T&M, Surveillance, Military & Aero, ...
all Markets for **Boards**

Telecom COTS World
Broadband Broadcast IoT Convergence

OEM Focus: Telecom IT, Networks, Data Centers, Cloud, Storage, Broadcast, Video Networks,
Service Providers: 850+

ATCA World

Advanced Telecom Computing Architecture (or AdvancedTCA, ATCA)
Standardized Platform for Carrier Grade Telecom Systems & Hi-end App's

e2mos
Embedded **E**xtreme **M**arketing & **O**pportunity **S**earch

Our Service is the Answer to your Biggest Challenge
Finding New Projects - New Customers and the Decision Makers

Made for Hi-end HW & SW VENDORS, based on 3 Decades Global Market Expertise

www.e2mos.com | Contact mgt@e2mos.com | Talk to us today, request a phone call