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

Mar-Apr 2018

You are one of those billions of connected things

Global IoT connected devices installed base in billions - 2015: 15 - 2020: 30 - 2025: 75

One billion US$ annually from 2017 onwards

Atos IoT partner for Coca-Cola Hellenic Bottling

IoT connected devices statistics

IoT security Hardware vs Software

Microsoft DICE enhanced security and unique device identification

ADLINK - Vortex DDS unique realtime large scale, complex transport management & connected vehicles

Nokia and EDF join forces to test IoT technology for industries

In this Edition

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

Your benefits:
- items selected for you
- you stay well informed
- easy reading
- many direct links for more
- No Time Waste
- FREE Worldwide

FREE Subscription
Click on the logos below

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

Our SERVICES Worldwide
- We search and we find New Business for you
- Fixing meetings with New Customers for you
- Biz Discovery Coaching
- Business Development
- Publications: we edit, you just need to supply good pictures
- e-mailings
- we own 250,000 qualified names Worldwide

Take a look at
www.e2mos.com

DICE offers enhanced security and unique device identification

January 22, 2018 -- By Dennis Mattoon, Microsoft Research

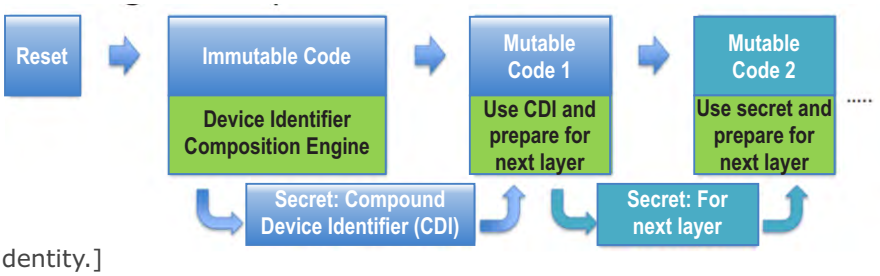
With the prevalence of connected devices, especially in Internet of Things (IoT) applications, embedded systems designers increasingly must contend with the types of trust and security issues that computing systems engineers have had to cope with for years.

The Trusted Computing Group (TCG) has a long history of developing standards-based trust technology to address these trust and security issues. And recently, the TCG has expanded its focus to include embedded systems. TCG's newly released Device Identity Composition Engine (DICE) architecture aims to provide enhanced security and unique device identification and attestation for the embedded space.

DICE relies on a combination of simple silicon capabilities and software techniques that work together to provide a cryptographically strong device identity. Improvements over software-only security are based, in part, on breaking the boot process into layers. Secrets unique to each layer and hardware configuration are created using a Unique Device Secret (UDS) known only to the DICE (and, optionally, manufacturer).

The device secrets and keys, unique to the device and each software layer, ensure that if code or configuration is modified, the secrets and keys will be different. With this approach, each software layer keeps the secret it receives completely confidential to itself. If a secret is disclosed through a vulnerability, patching the code will automatically re-key the device. Figure 1 shows how trusted code in DICE provides a hardware-based root of trust for the platform. In the DICE boot model:

1. Power-on unconditionally starts the DICE
2. DICE has exclusive access to the UDS
3. Each layer computes a secret for the next layer (via a cryptographic one-way function)
4. Each layer protects the secret it receives



[Figure 1 | Using new secrets at each layer, the DICE model builds upon trusted immutable code to build a trust chain and provide strong device identity.]

Hardware, with features to limit access to the UDS only to the DICE, performs the initial step for DICE security. Both the UDS and the measurement of the first mutable code that runs on the DICE platform, where DICE provides the root of trust for the measurement, are used to compute the Compound Device Identifier (CDI). Starting with the CDI, each successive software layer uses the secret and a measurement of the next layer to derive a new secret for the following layer. Each layer must erase its own secret before transferring control. This process continues during startup, resulting in a measurement chain that is rooted in the device's identity and based on measured code.

For a real-world look at this technology, Microsoft's Robust Internet of Things (RIoT) architecture provides a reference implementation for leveraging DICE. This is the same architecture that underpins the Device Provisioning Service in Azure IoT. In the RIoT reference, a DICE-enabled processor runs a first-stage bootloader called RIoT Core. RIoT Core is responsible for deriving the device identity based on measurements performed by the DICE. RIoT Core then combines its own measurement of device firmware with the CDI it received form the DICE and passes this secret value to firmware so it may further derive its secrets and keys.

In this architecture, device firmware relies on attestation (the cryptographic reporting of the security configuration of a device) elements encoded in a cryptographic hash value called the Firmware Identity (FWID). The FWID is the hash of the Firmware Security Descriptor (FSD) that together with the UDS are simulated inputs to a function that derives the DICE-based identities and certificates.

There are three basic requirements for implementing a DICE platform. These include:

1. The ability to compute a hash (ideally in hardware or ROM),
2. A UDS of at least 256 bits,
3. A protection mechanism that limits access to the UDS to the DICE exclusively and only resets on platform reset

These characteristics are typically found in available microcontrollers (MCUs) used in embedded applications, but MCUs specifically designed for the DICE architecture can optimize their implementation. Hardware available to implement the DICE architecture includes existing MCUs: STMicroelectronics' STM32L0\L4 family of MCUs, Micron Technology's Authenta-based flash memory. New MCUs specifically designed for DICE include Microchip Technology's CEC1702 with a SecureIoT1702 Demo board and flash memory from WinBond.

With the DICE specification nearing finalization, even more design-in tools and support will be available from a broader range of suppliers.

Dennis Mattoon is a Senior Software Development Engineer for Microsoft Research. As one of the founding members of the Security and Privacy Research and Engineering team in MSR, Dennis and his team have spent the last 10 years focused on advancements in trusted computing and system security. His most recent work has been on the creation of the Device Identifier Composition Engine Specification and Architectures (TCG DiceArch), Robust and Resilient IoT (RIoT), and the Cyber-Resilient Platform Initiative.

Alstom reinforces its digital offering with the acquisition of 21net, expert in onboard internet

Alstom has signed a purchase agreement for the acquisition of 21net, from the Innovacom fund and other investors. 21net is a provider of on-board Internet and passenger infotainment for the railway industry. Its on-board connectivity solution is based on multiple technologies such as satellite, cellular and high-speed wireless from trackside antennas. The company is headquartered in the UK with subsidiaries in Belgium, France, Italy and India. It employs 50 people and its turnover represented around 16 million in 2017.

Founded in 2001, the company has developed over the years an expertise in end-to-end network design and optimization for broadband Internet on high-speed trains. The company notably installed Wi-Fi equipment for high-speed trains in France with a contract signed with SNCF in 2016. Alstom has already worked with 21net on the Wi-Fi and infotainment equipment of the NTV train fleet in Italy.

This new acquisition, one year after that of Nomad Digital, will reinforce Alstoms digital offering and expertise. The demand for seamless connectivity throughout passengers journey is today a must. Alstom will support operators in the acceleration of digital trends worldwide declares Jean-François Beaudoin, Senior Vice-President for Digital Mobility at Alstom.

Innovacom has been pioneering the development of new technologies through start-ups and then consolidating them within leading companies for 30 years. We are pleased with this new concretization of the open innovation process to the benefit of all parties, adds Vincent Deltrieu, Partner at Innovacom.

The closing of the transaction is expected in one month from now. Alstom will begin integrating 21net into the Group from then.

Sensor Systems: Fundamentals and Applications

by Clarence W. de Silva

Features

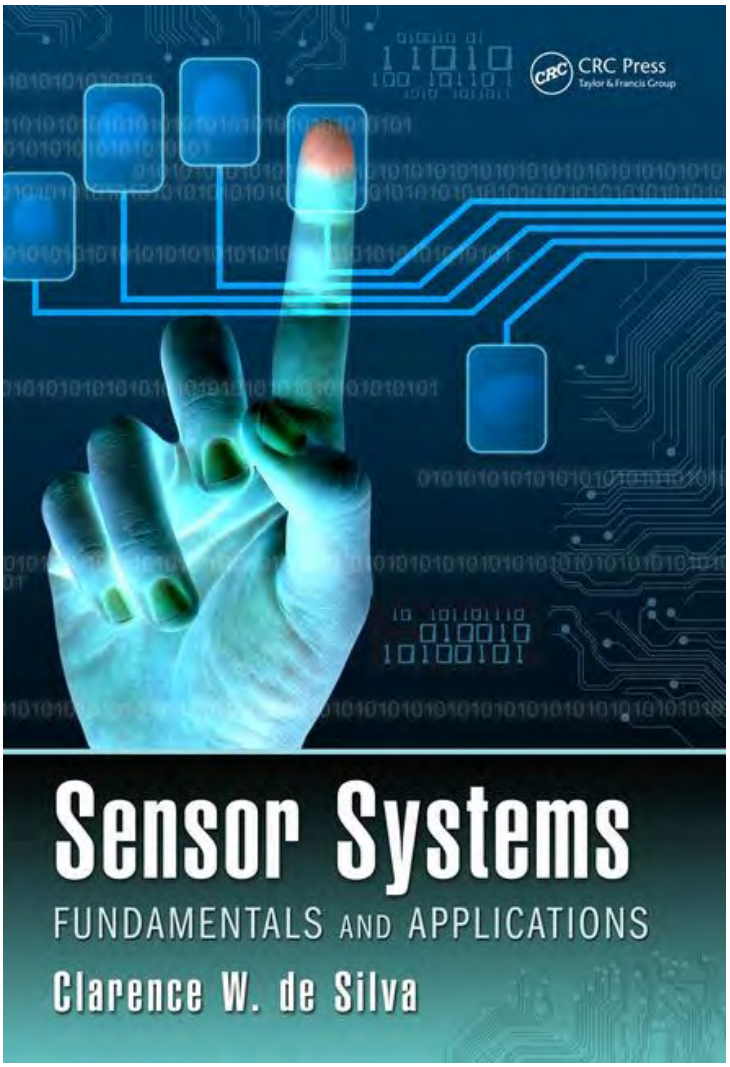
Presents physical principles and analytical methods for sensors using simple mathematics
Contains material that is appropriate for mechanical, aerospace, and electrical engineering courses
Covers wireless sensor networks, MEMS sensors, and multi-sensor data fusion
Gives practical procedures for the design, selection, and integration of sensors
Includes complete solutions manual, tutorials, and PowerPoint slides with text

Summary

This book covers sensors and multiple sensor systems, including sensor networks and multi-sensor data fusion. It presents the physics and principles of operation and discusses sensor selection, ratings and performance specifications, necessary hardware and software for integration into an engineering system and signal processing and data analysis. Additionally, it discusses parameter estimation, decision making and practical applications. Even though the book has all the features of a course textbook, it also contains a wealth of practical information on the subject.

Buy the Bookfrom Amazon: CLICK HERE

More books from Clarence W. de Silva: CLICK HERE



Atos recognized as a global Leader in IoT Services by Everest Group

January 15, 2018 05:18 ET | Source: Atos International

Paris, January 15 2018 - Atos, a global leader in digital transformation, today announces it has been named a global Leader by Everest Group in its latest report: IoT Services PEAK Matrix(TM) Assessment and Market Trends 2017: Have You Taken the Plunge in IoT Yet?[i]. The report assesses the relative capabilities of 18 global IT service providers offering IoT Services. **Atos' System Integration and Operations capabilities and Worldline's ready-to-use solutions and are recognized for enabling clients to progress rapidly from PoC to production.**

In the report, leaders are 'delivering strategic value to their customers' which 'forms the core of their value proposition and a futuristic approach for IoT services development roadmap is witnessed' and have 'led their customers through large scale transformation journeys powered by IoT'.

"We witness a 25% increase in IoT pilot projects moving to production stage, and Atos' consulting driven engagement model has further supported its customers to progress from POC to production stage rapidly and to achieve concrete business results. Additionally, Atos' investments in R&D and strategic partnerships across the IoT stack together with Worldline's ready to use solutions has enabled it to deliver innovative and secure IoT solutions across different industries." said Yugal Joshi, Practice Director, Everest Group.

Elaborating on Atos' role as a leader in IoT, Dominique Grelet, Global Head of **Atos Codex IoT Services** at Atos said: "We are proud to be recognized as a global Leader in IoT Services by Everest Group. This validates our ability to effectively leverage agile processes, innovative tooling and automation, while working with our extensive IoT partner ecosystem, to deliver, manage and secure the full IoT value chain from connected devices to edge computing to the datacenter."

These IoT services combine Atos' horizontal connectivity and platform services, such as the platforms delivered by Worldline, European leader in the payments and transactional services industry and an Atos company, and partner platforms such as **Amazon Web Services** and **Microsoft Azure**, with advanced, (vertical) business-driven analytics, apps and use cases, enable customers to securely transform data into reliable business value in every market.

The deep integration with company processes - such as ERP (Enterprise Resource Planning) and PLM (Product Lifecycle Management) - is a key differentiator as it gives Atos the ability to take end-to-end responsibility.

To download the report, please go to http://go.atos.net/LP=568.

About Atos

Atos is a global leader in digital transformation with approximately 100,000 employees in 72 countries and annual revenue of around € 12 billion. European number one in Big Data, Cybersecurity, High Performance Computing and Digital Workplace, the Group provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies, digital expertise and industry knowledge, Atos supports the digital transformation of its clients across various business sectors: Defense, Financial Services, Health, Manufacturing, Media, Energy & Utilities, Public sector, Retail, Telecommunications and Transportation. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline. Atos SE (Societas Europaea) is listed on the CAC40 Paris stock index.

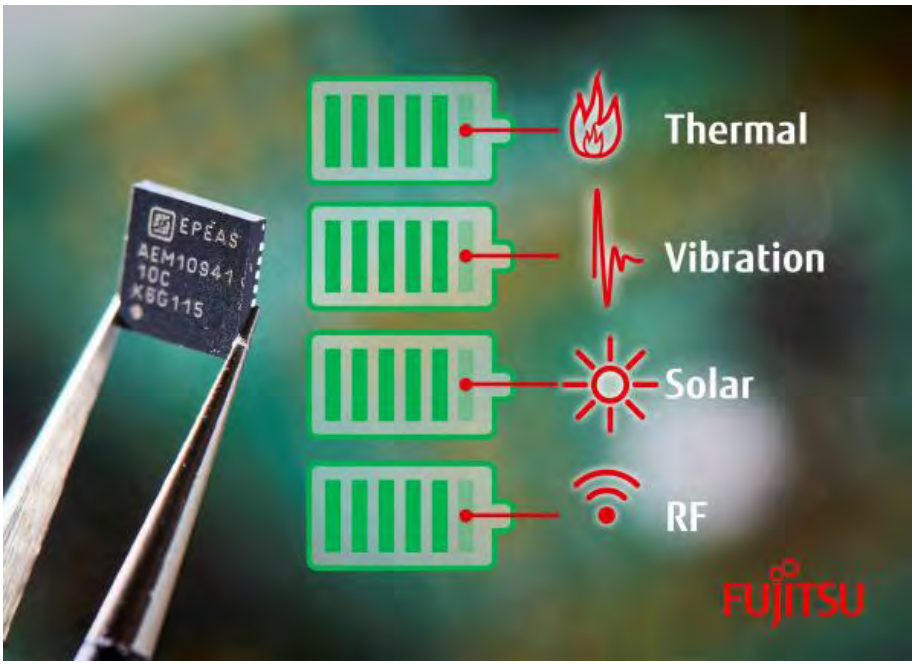
Press contact:
Laura Fau | laura.fau@atos.net | +33 6 73 64 04 18 | @laurajanefau

Atos is active in the followong Industries

AEROSPACE
AUTOMOTIVE
BANKING
CENTRAL GOVERNMENT
CHEMICALS
CONSUMER PACKAGED GOODS
DEFENSE
DISCRETE MANUFACTURING
EDUCATION
ENERGY
HEALTHCARE
HOSPITALITY
INSURANCE
LIFE SCIENCES
LOCAL GOVERNMENT AND CITIES
MEDIA
RETAIL
SPORTS & MAJOR EVENTS
TELECOMMUNICATIONS
TRANSPORT
UTILITIES

Fujitsu adds energy-harvesting components from e-peas

Published in eeNews Embedded February 19, 2018 // By Ally Winning



Fujitsu Electronics Europe (FEEU) is expanding its linecard with products from e-peas that support a wide range of energy sources such as photovoltaic, thermal, vibration or RF.

Available now is the AEM10940, and this will be followed by the AEM10941 and AEM30940. The components have an ultra-low-power boost converter, with an efficiency of up to 94%, and voltage reference, power management and LDOs integrated, which means they do not require a significant amount of external components. The devices also have a cold start feature that requires an input voltage of only 380 mV.

The energy harvesting devices will compliment FEEU's existing range of low-power products that include FRAM as well as Ambiq Micro's MCUs, RTCs and BLE solutions.

Fujitsu: http://www.fujitsu.com/feeu/ **e-peas:** https://e-peas.com/

Related news

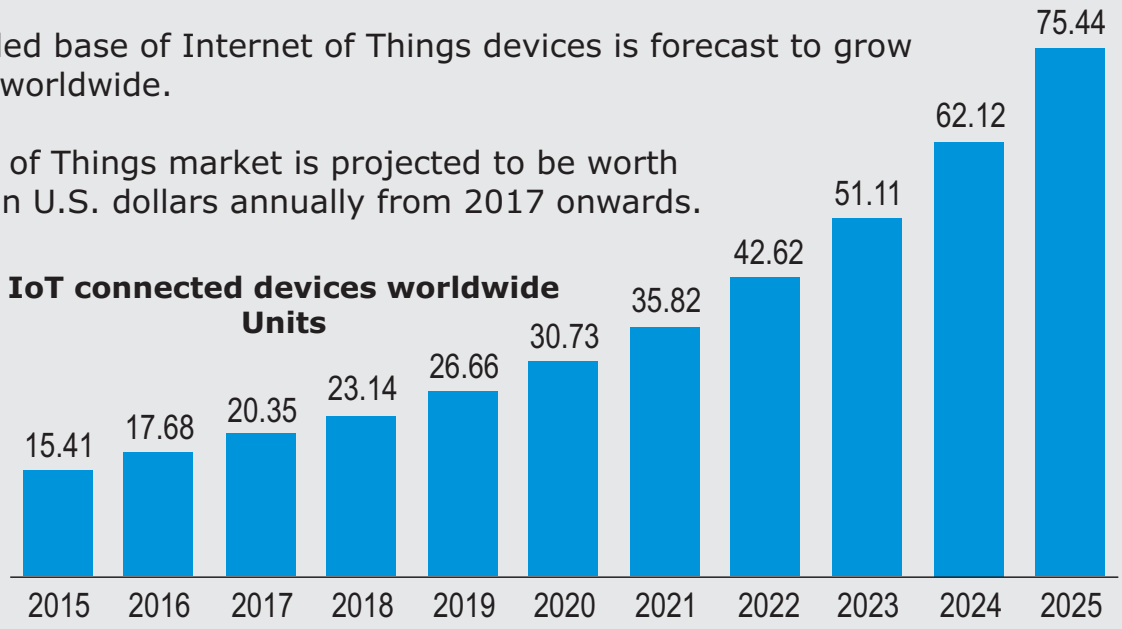
BluetoothLE & energy harvesting sensor shields extend IoT dev kit
Lemonbeat updates Studio software for IoT endpoint development
Evaluation kit eases energy harvesting power management design
Solid-state battery – a hybrid of battery and capacitor

Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)

Source: Statista

For 2020, the installed base of Internet of Things devices is forecast to grow to almost 31 billion worldwide.

The overall Internet of Things market is projected to be worth more than one billion U.S. dollars annually from 2017 onwards.

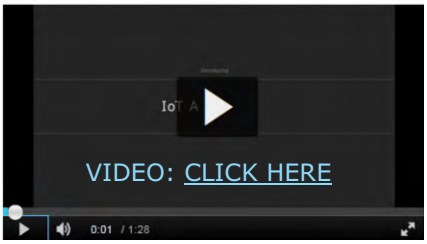


IoT Accelerator platform by Ericsson

Moving your IoT concepts from "how?" to right now

IoT Accelerator - Turning really good concepts into concrete realities

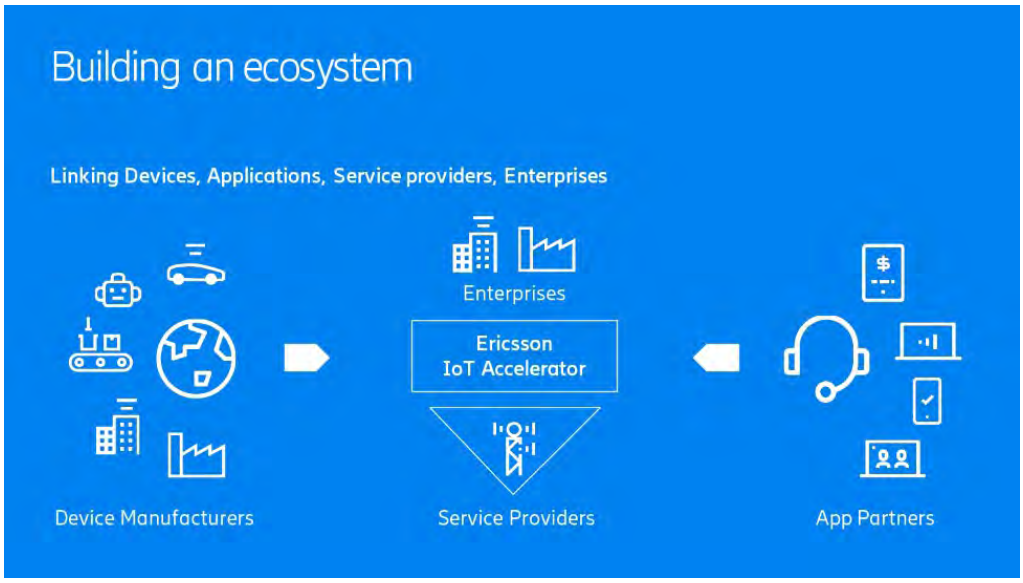
When planning your IoT offerings, translating your IoT dreams to the real world of business can be complex. So we make it easy with the Ericsson IoT Accelerator, your universal translator for app developers, device manufacturers, device onboarding, or monetization matters. We transform all tongues, turning your IoT concepts into a concrete reality - all so you can talk tomorrow's big business.



IoT Accelerator - pick and choose to match your needs

The IoT Accelerator Platform has built in modules, enabling you to customize it exactly to your needs.

IoT Accelerator - The middleman that doesn't meddle



Our goal with IoT Accelerator is to add value to the ecosystem. With our full stack IoT platform, you'll benefit from faster time-to-market, lower startup costs, and easy scalability based on an aaS model. Together with data and device management, monetization, analytics, security, and our industry-leading know-how in connectivity, IoT Accelerator will be the first middleman you love.

IoT Accelerator Platform's key functionalities

The IoT Accelerator platform is built to connect billions of devices and millions of applications easily and seamlessly.

Quick onboarding, quicker to market
Device and Data Management with zero-touch onboarding and lifecycle management.

Billions of things, one easy way to manage
World-class connectivity management for billions of devices.

Global ecosystem, global possibilities
Building the IoT ecosystem with enterprise administration, developer and partner onboarding and API exposure.

Orchestrate, integrate, automate
Analytics, data storage, monetization engine and security.

Key benefits

Guaranteed performance
A SLA guarantees you functionality and capacity at all times.

Pay only for what you use
Built as a Service, our platform grows with your business.

Scalable and secure
Data protection, privacy and integrity are ensured as your business scales.

Technology made easy
We take care of the technology, so you can focus on your customers.

Learn the details around Ericsson IoT Accelerator: https://www.ericsson.com/ourportfolio/iot-solutions/iot-accelerator

ADLINK Announces Support for SGeT's Universal IoT Connector (UIC) Specification and Real-time XRCE Device Data-Connectivity

Complementing SGeT's UIC with XRCE middleware for high-performance Device-Fog-Cloud Computing is just one more example of ADLINK 'Leading EDGE COMPUTING'

Mannheim, Germany -- 21 Feb 2018 -- ADLINK Technology, Inc., a global provider of advanced Edge Computing products, today announced its support for the Standardization Group for Embedded Technologies' (SGeT) specification for a Universal Internet-of-Things Connector (UIC). In addition, ADLINK also announced advanced embedded middleware support that complements the UIC, with a 'plug-in' for XRCE real-time data distribution.

Together, these two open-source software enhancements for ADLINK's embedded products portfolio bring embedded computing firmly into the IoT arena, by enabling device-to-device and device-to-Cloud data connectivity - with standards-based inter-operability and performance levels never before possible with commercial-off-the-shelf (COTS) products.

The UIC is SGeT's first software-only standard. It supports the comprehensive roll-out of IoT applications by standardizing embedded hardware connectivity for Edge and Cloud Computing. Before UIC, all hardware I/O communication had to be done manually for each-and-every Edge and Cloud connection. This obviously created significant challenges for embedded hardware deployment, support and upgrade in distributed computing (e.g., IoT) systems.

Through the UIC, the integration of distributed devices is made easier via three levels of abstraction/partitioning. The UIC makes a distinction between: 1/ the device configuration (hardware identification, device mapping, value-to-information matching), 2/ the sensor and actuator communications (hardware driver), and 3/ the device communications (data transfer and processing). With more than 500 Cloud service offerings, and an even greater number of possible hardware configurations, this provides a very open, practical and efficient approach to building, deploying, maintaining and evolving IoT systems (i.e., integrated device-Edge-Cloud Computing).

The UIC will, out-of-the-box, support communications to hardware devices through the established Embedded API (EAPI) PCI Industrial Computer Manufacturers Group (PICMG®) standard. This means that the whole ADLINK product portfolio of Computer-on-Modules (COM) and embedded boards will be able to leverage the UIC.

In addition to UIC support for its portfolio of devices, ADLINK is also announcing support for a XRCE data-connectivity 'plug-in', which leverages the UIC to provide high-performance peer-to-peer data communications between devices. XRCE stands for 'eXtremely Resource-Constrained Environments' and is a derivative of the Object Management Group's (OMG) open-standard Data Distribution Service (DDS) specification. XRCE complements other IT and OT data protocols (e.g., MQTT and OPC/UA) but provides the more advanced real-time data-connectivity required for performance-critical distributed systems (e.g., the deterministic data delivery required for distributed robotics, autonomous vehicles, defense systems, etc.).

Furthermore, UIC and XRCE support the embedded computing industry's requirement for dual-sourcing (with interoperability and exchangeability), that is, all modules and subsystems interoperating in a seamless way without vendor-specific knowledge. This supports important cost, time-to-market and risk-reduction initiatives by OEMs through, for example, reducing vendor lock-in and improving application code portability.

These initiatives are just one more example of ADLINK 'Leading EDGE COMPUTING'. ADLINK has extensive experience in distributed computing from the sensor to the Cloud (e.g., its 2015 acquisition of PrismTech), and its focus on and expertise in Edge Computing (which is effectively connected embedded computing) is exceptional, and possibly unique, within the SGeT membership.

ADLINK will showcase its UIC/XRCE capabilities in a device-Fog-Cloud Computing demonstration at Embedded World 2018 in Nuremberg, Germany, Feb. 27 to March 1 (booth 1-540).
"We're very pleased to collaborate with embedded computing standards organizations such as SGeT," said Edgar Chen, general manager, Embedded Platforms and Modules, ADLINK. "Our developments in UIC connectivity and XRCE data communications provide our embedded computing customers with new opportunities to offer leading-edge IoT solutions. For ADLINK, Edge Computing is connected embedded computing, so pioneering connectivity solutions for embedded systems is a strategic priority for us."

For more information on SGeT's UIC please visit:
https://www.sget.org/news/view/article/universal-iot-connector-open-standard-connects-embedded-devices-to-the-cloud.html

Discover ADLINK IoT Products & Solutions

New medical venture is dedicated to wearable biometric solutions

SOURCE: eeNews Embedded - March 07, 2018 // By Ally Winning Click Here

Semiconductor Ideas to the Market (ItoM) B.V. has launched a sister company, which will be dedicated to developing wearable biometric solutions for the medical field.

The new company will build on ItoM's work over the previous five years in designing solutions and algorithms for electrophysiological diagnostic and monitoring systems (electrocardiography, electroencephalography, electromyography, respiratory, etc.).

ItoM Medical's biometric solutions will be targetted at medical grade equipment, as it has been slower to advance than the personal health market, which mainly relies on trolley-based systems. The new company will develop solutions that are less bulky, offer medical grade accuracy and be less stressful on patients.

The new company will look to assist medical device manufacturers by offering small form factor electronics that feature low-power consumption, algorithms and hardware and software design services. ItoM Medical will also provide a CE pre-certified embedded platform for wearable ExG diagnostics and monitoring systems.

More information: https://www.itom-medical.com

Related news:

Flexible tactile actuator for wearable haptics
Human-eye resolution VR/XR headset uses Milbeaut image signal processing
Biomedical sensors combine with stretchable display for skin electronics
Micro-display for VR and AR wearable products

Nokia and EDF join forces to test Internet of Things technology for industries

- Project led by R&D division of EDF, will explore low power, wide area (LPWA) wireless technologies to support safe and secure connections with potentially millions of sensors and other devices
- Joint effort incorporating Nokia TestHub services is among the industry's most comprehensive testing to date using IoT devices for industries
- Represents key step in EDF's move towards the use of IoT; highlights Nokia's role as a key partner for the deployment of networks for industries

Espoo, Finland - 06 Feb 2018 - Nokia has been selected by French power utility EDF's R&D unit to test the performance of LPWA wireless networking technologies - key emerging standards for Internet of Things (IoT) device connectivity - to support critical operations for industries. The two companies will engage in a comprehensive testing regime, among the first of its kind in the industry, exploring the capabilities of LPWA technologies to support real-world industrial applications. Nokia is EDF R&D's exclusive partner for this effort.

EDF R&D will utilize Nokia TestHub Services in Nokia's Device Testing Lab in France - which gives customers access to state-of-the-art, carrier-grade wireless infrastructure - when testing IoT/M2M objects, chipsets, modules and user devices across all wireless technologies and frequencies. This enables devices to be tested on real network infrastructure rather than a simulated network, which reduces guesswork in testing and analysis and minimizes risks in advance of widespread commercial introduction.

The testing will compare IoT technologies recently standardized by the 3G Partnership Project (3GPP) - including NarrowBand-IoT (NB-IoT) and LTE-Machine (LTE-M) (also known as enhanced Machine-Type Communications or eMTC) - with other emerging, largely unlicensed IoT technologies.

This agreement builds on Nokia's strong track-record providing mission-critical networks toindustries, and highlights the company's strong position in the emerging market for IoT connectivity. It also highlights the progress of Nokia's strategy of expanding its customer base outside of the traditional telecommunications sphere, a key focus of the company's diversification efforts.

Stéphane Tanguy, head of IT Systems, EDF R&D, said: "The Internet of Things offers tremendous opportunities for our group. Many use cases can be enabled by IOT technologies in various businesses from power generation to marketing. As the R&D engine of the EDF Group, it is our responsibility to characterize the objects, their connectivity, their integration into IoT platforms and the related end-to end cybersecurity properties. Among the connectivity solutions, it is essential that we understand the performance, the maturity and the adequacy of each technology for our different use cases by an objective and agnostic approach. The cellular IOT technologies (LTE-M and NB-IOT) are two major technologies that we have decided to test with Nokia, which provides us with a very interesting test environment and valuable expertise to carry out these evaluations."

Matthieu Bourguignon, head of Global Enterprise and Public Sector, Europe, for Nokia, said: "The use of IoT devices in industrial networks is in its infancy, but given the expected huge numbers of devices that will be deployed in the future, it is critical that our customers can evaluate now the various technologies before making substantial investments. Nokia's Device Testing Lab, staffed by some of the most experienced wireless networking experts in the industry, will make it much easier for EDF to evaluate the performance of LPWA against other emerging technologies and reduce the risk of future deployments."

About EDF

A key player in energy transition, the EDF Group is an integrated electricity company, active in all areas of the business: generation, transmission, distribution, energy supply and trading, energy services. A global leader in low-carbon energies, the Group has developed a diversified generation mix based on nuclear power, hydropower, new renewable energies and thermal energy. The Group is involved in supplying energy and services to approximately 37.1 million customers, of which 26.2 million in France. The Group generated consolidated sales of ☐71 billion in 2016. EDF is listed on the Paris Stock Exchange.

About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry's most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. www.nokia.com

IoT security: hardware vs software

Bonnie Baker (see below) -January 17, 2018

We are now in the business of connecting everything to everything. And with this, the Internet of Things (IoT) is born. Once this total connectivity is accomplished, the collective effort this brings lets us start the next string of new and exciting systems. This results in massive amounts of data that must be trusted and processed (Figure 1).

Figure 1
With the IoT, the availability of information is at your back door

But, as they say: "buyer beware." This is all good, but total connectivity opens the opportunity for unintentional or malicious data corruption and contamination to occur. Cryptographic methods can be applied to resolve these vulnerabilities. A decision that system designers face is deciding between software-based or hardware-based security solutions. Both technologies combat unauthorized access or modification to data; however, their differing features bear further examination before making the final selection.

Software-based security
Utilizing existing system resources, software security systems were the first to show up in the marketplace. These solutions are relatively inexpensive, as they share resources to protect and safeguard data with other programs in the system. An additional capability of a software-based implementation is the ability to revise and upgrade security as threats and vulnerabilities evolve.

A software security system places a load onto a host processor. Potentially, this could compromise the overall system efficiency. Beyond these concerns, the software approach is the weak link within systems-security architecture. Secrets remain vulnerable to discovery and the algorithms typically run on general-purpose non-secure hardware and are similarly an attack risk.

With all this said, cost-effective, software-based security can be effective in physically secure environments, preventing unauthorized access to the system.

Hardware-based security
Hardware-based security uses a dedicated integrated circuit (IC), or a processor with specialized security hardware, specifically designed to provide cryptographic functions and protect against attacks. Security operations, such as encryption/decryption and authentication, take place at the IC hardware level where crypto algorithm performance is optimized. Additionally, sensitive information, such as keys and critical end-application parameters, are protected within the electrical boundary of crypto-hardware.

The security IC contains circuit blocks such as a math accelerator, random number generator, nonvolatile memory, tamper detection, and a physically unclonable function (PUF). The PUF block is particularly interesting in that it has a unique characteristic of being immune to invasive or reverse-engineering attempts to extract sensitive data such as a cryptographic key. The Maxim DS28E38 is an example of a security IC that integrates PUF, both to generate keys and to protect against invasive security attacks.

It is incredibly difficult and expensive to alter silicon; therefore, cybercriminals are deterred from attacks on hardware-based security. Further, when attacked, the security IC is capable of shutting down operations and destroying sensitive data before being compromised. Such a solution may be a little more expensive, but it provides a dramatic reduction in the risk of unauthorized access to embedded devices, peripherals, and systems.

Hardware-based security is very effective in all application environments, especially those where the end equipment is exposed and physically accessible to the bad guys.

Buckle your seat belt
Overall, security can be a complex subject. But it is one that must be addressed and embraced to prevent bad things from happening to an end product such as an IoT device. Software-based security is an option, but the path to comprehensive and reliable security is to select a hardware-security alternative.

Bonnie Baker has been working with analog and digital designs and systems for more than 30 years, and is writing for Maxim.

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.