FREE Download www.iotworld.be

IoT World

Internet of Things from A to Z

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

IoT World is a Global Publication of e2mos

May 2016

In this issue

Security by design from day ONE, not security as an add-on the last minute

This is Key to Success

Statement collected
by Daniel Dierickx
from prominent IoT players

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

KORE Wireless Group Completes Acquisition of Wyless Group Holdings

KORE Wireless Group, Inc. is the world's largest managed wireless network services provider specializing in M2M communications and the IoT

ATLANTA and BOSTON —April 13, 2016— KORE Wireless Group, Inc. (“KORE”), the world's largest managed wireless network services provider specializing in Machine-to-Machine (M2M) communications and the Internet of Things (IoT), today announced that it has completed the acquisition of Wyless Group Holdings (“Wyless”).

The all-cash transaction closed on April 11, 2016, following the clearance of regulatory requirements. Financial terms are not disclosed. For more information visit: www.wyless.korewireless.com

+6M
Active
Devices

+3000
Customers
Served

110
Countries
Leading
Carriers

The combination of KORE and Wyless creates the only truly global, independent multi-platform Internet of Things (IoT) services company.

Delivering an unprecedented portfolio of connected technology, location-aware solutions and global innovations including e-SIM services, the company's scope and scale will provide customers and partners the benefits of a more diverse, global, footprint and access to an award-winning set of service platforms to support complex end-to-end managed data solutions.

About KORE Wireless Group

KORE provides the connectivity and services that make the Internet of Things possible. Founded in 2003, KORE is the worlds' largest managed network services provider specializing in Internet of Things (IoT) and Machine to Machine (M2M) markets. KORE provides the critical wireless connectivity empowering application, hardware and wireless operator partners to rapidly bring new IoT and M2M innovations to market, with millions of active on-network units in more than 110 countries. KORE delivers choice, reliability and global native coverage through multi-carrier and Tier 1 carrier cellular and satellite network services – including LTE, GSM and CDMA - as well as advanced applications to easily manage IoT connected devices. KORE Position Logic software provides seamless location-based services (LBS) for businesses. For more information, visit www.koretelematics.com, read the KORE blog and connect with KORE on LinkedIn, Google+, Facebook, Twitter, YouTube and Vimeo.

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

Dear Reader,

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

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

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

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

Our WORLDWIDE Services include:

- Business Discovery
- Customer Meeting Setup
- Telemarketing
- Call Campaigns
- e-mailings Worldwide
- and our four magazines, each magazines has its own Website (see page 7)

It is all based on:

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

More www.e2mos.com

Thank you.

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

Industry Leaders ADLINK, PrismTech, IBM and Intel to Host IoT Innovation Day on June 9 in San Jose, CA

Registration underway for event designed to provide new strategies to companies developing and deploying Industrial IoT systems and Edge Computing

San Jose, CA, USA – May 26, 2016 – ADLINK Technology, Inc., a leading global provider of Industrial Internet of Things (IIoT) platforms, in collaboration with PrismTech (an ADLINK company), IBM and Intel, will host an IoT Innovation Day at The Tech Museum in San Jose on June 9th from 2 – 5 pm, with a cocktail reception to follow. The companies will share strategies and key insights and lead open discussions targeted at helping businesses embrace the benefits of IIoT computing on the edge — paving the way for the shift from the connected device to the intelligent device.

The event will detail how Edge Computing is changing the way IoT systems are built, enabling a new generation of low latency, intelligent analytics that can process and act on intelligent device-generated data in real-time. Among the keynote speakers for the IoT Innovation Day are PrismTech Founder Keith Steele, IBM Global Innovation Executive Rob Risany, Intel IoT Group Chief Technology Officer (CTO) Brian McCarson, ADLINK CTO Jeff Munch and PrismTech Chief Solutions Architect Toby McClean. Presentation topics will address the changing IoT landscape, the impact of Moore's Law on IoT and computing on the edge.

“For attendees, this is an exceptional opportunity to arm their businesses with cutting-edge strategies and insights into IoT systems and edge computing,” said Steele. “This will help elevate these companies to the next level of IoT computing.”

In addition to the presentations and open discussions, IoT Innovation Day will also feature a live demo of ADLINK's PMQi predictive maintenance and quality platform, which features IBM PMQ business analytics software, Intel® technology and PrismTech's Vortex Data Distribution Services (DDS), as well as a panel discussion related to use cases, testimonials and partnering opportunities.

The Tech Museum of Innovation is located at 201 South Market Street, San Jose, California. For more information and to register for the event, please visit: https://iotinnovationday.splashthat.com/.

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

ADLINK is a Premier Member of the Intel® Internet of Things Solutions Alliance and is active in several standards organizations, including PCI Industrial Computer Manufacturers Group (PICMG), PXI Systems Alliance (PXISA), and Standardization Group for Embedded Technologies (SGeT).

ADLINK is a global company with headquarters in Taiwan and manufacturing in Taiwan and China; R&D and integration in Taiwan, China, the US, and Germany; and an extensive network of worldwide sales and support offices. ADLINK is ISO-9001, ISO-14001, ISO-13485 and TL9000 certified and is publicly traded on the TAIEX Taiwan Stock Exchange (stock code: 6166).

Securing the Internet of Things

An Architect's Guide to Securing IoT Devices Using Hardware Rooted Processor Security

A White Paper from Synopsys
Author: Ruud Derwig, Senior Staff Engineer

Abstract

The Internet of Things (IoT) is undeniably a hot topic right now, but there are also many definitions of what an IoT device is exactly. One of the common requirements that seems to be universal is the need for security. Although it includes functional aspects, security — or rather, lack of security — is an emerging system property that cannot simply be realized by integrating a single, magic security IP block into your system. This paper provides an overview of security basics, feature requirements, technical solutions, and associated system-level trade-offs for implementing security in IoT devices. Making the required trade-offs is significantly easier by leveraging secure, proven building blocks that were designed with secure systems in mind and optimized for low footprint and energy. Given the insights of this paper, trade-offs for a specific IoT device can be made more easily, the optimal mix of features can be decided on, and the resulting secure architecture can be implemented efficiently.

Introduction

IoT products like smart home controllers, wearables and smart metering devices bring many benefits such as improved convenience, better health or environmental savings. But the Internet connectivity and massive data collection that enable these benefits also bring threats to the reliable functioning of these products and to the privacy of their users.

When architecting a system, trade-offs have to be made. This is especially true with security, as there is no one magic solution that makes a system "secure". The trade-offs to be made are complex, inter-dependent, and span multiple disciplines. Hardware versus software, throughput versus area and energy consumption, and security level versus cost are some of the decisions to be made. But although the magic IP block that protects a full system does not exist, securing an IoT system is made significantly easier by using building blocks that were designed with secure systems in mind.

IoT end-to-end systems can roughly be classified into three groups, as shown in Figure 1:

- The endpoints interacting with the physical world (edge devices)
- Hubs and gateways that connect to edge nodes for data aggregation and that also act as gateway to other, larger area networks
- The cloud with remote (big) data storage and servers for processing the data collected by edge devices

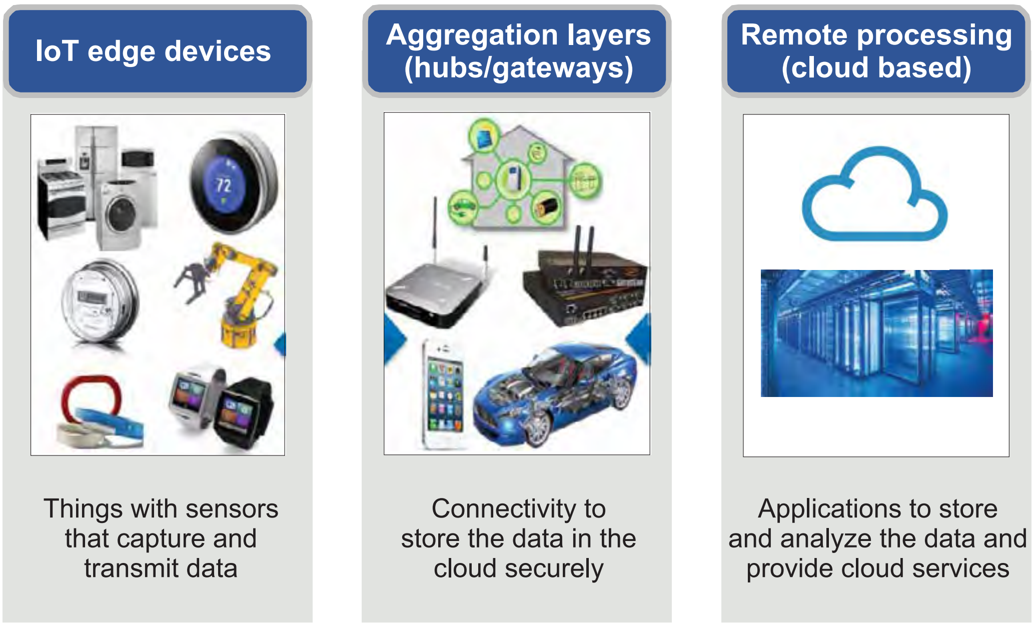

IoT edge devices
Aggregation layers (hubs/gateways)
Remote processing (cloud based)
72
Things with sensors that capture and transmit data
Connectivity to store the data in the cloud securely
Applications to store and analyze the data and provide cloud services

Figure 1. IoT end-to-end system overview

IoT systems security should always be considered end-to-end. But since there is a significant data size, speed and power variation across the different devices in the chain, as well as different security threats, technical solutions for the groups of devices differ as well. In this paper we focus mainly on the lines of security defense that are relevant to the edge nodes and peripherally consider aggregation and gateway nodes.

... to next page

Securing the Internet of Things ... from previous page

Security Basics

We'll start with an overview of general security aspects and some trends. Security is about confidentiality, integrity and authentication. Confidentiality aims to prevent information leakage to parties that should not have access to that information. Integrity is about ensuring that the information itself is original and has not been tampered with. Authentication ensures that the identities of the parties producing and consuming the information are uniquely established. Sometimes two other aspects are added, non-repudiation and availability. Non-repudiation uses cryptographic tools to prove that a unique user has made a transaction request. It must not be possible for the user to refute his or her actions. Availability, strictly speaking, is more of a safety or robustness requirement, but it touches on security as well through denial-of-service attacks that prevent proper functioning of an IoT device, for example.

To achieve the above security properties, over the last decades a number of foundation technologies have been developed that are continuously being enhanced. First of all, there are cryptography algorithms. These are the cornerstone of any secure system and include functions for encryption/decryption (e.g. AES [1] or ECC [2]) and cryptographic hashing (e.g. SHA-2 [3]). Encryption and decryption implement confidentiality, and use (partially) secret keys that should be protected against unauthorized access or use. Cryptographic hash functions are used for message integrity. They compute a checksum that is nearly impossible to reconstruct without the original message.

For authentication, typically a combination of hashing and encryption is used with either shared secret keys or using public key infrastructure (PKI) like X.509 certificates [4]. The next foundation technology is built on top of these cryptographic algorithms: higher-level protocols like secure http (https) connections (e.g. using TLS [5], secure payment transactions (e.g. based on EMV standards [7]), but also protocols for secure over-the-air software upgrades (e.g. OMA-DM [8]). The third foundation technology is platform security. Platform security is not about protecting sensitive contents, it is about protecting the actual device or platform that stores and processes these contents so it can be trusted. The protection can range from physical protection, such as a closed box with no external access to memories storing secret keys, to software protection against malware and sandboxing non-trusted applications. Platform security starts with a so called root of trust that provides an identity that cannot be tampered with. Building on this trusted starting point, a processor can securely boot and then load and verify application software before starting to execute it.

When designing secure systems, the first task is to identify the security requirements. A good way to identify these is to perform threat analysis and modeling. By investigating system use-cases, environment, main components and the system interfaces with respect to the information to be protected, a list of potential attacks can be created. For each attack, a number of attributes should be considered in order to assess the risk and reward of the attack and consequently the priority and budget for countermeasures. These attributes may include the cost and availability of the equipment required for the attack (a laptop with Wi-Fi, or a focused 3 ion beam (FIB) device), the consequences of the attack (a single device compromised, or a full class of devices sharing the same key), but also the scalability of an attack (requiring physical access to the device, or an attack over the Internet).

IoT Security Threats and Attacks

A good source for 'traditional' Internet connected device attacks is the Open Web Application Security Project (OWASP [9], [10]). OWASP lists the following as the top 10 vulnerabilities for IoT systems:

- Insecure Web Interface
- Insufficient Authentication/Authorization
- Insecure Network Services
- Lack of Transport Encryption
- Privacy Concerns
- Insecure Cloud Interface
- Insecure Mobile Interface
- Insufficient Security Configurability
- Insecure Software/Firmware
- Poor Physical Security

Download the 16 pages White Paper Click Here

... in addition to these 2 pages it includes:

IoT Security Countermeasures
System-level protection mechanisms
Processor-level protection mechanisms
Software level protection mechanisms
Example and Conclusion
References: 30 items

SYNOPSYS®
Silicon to Software™
www.synopsys.com

The IoT needs fog computing

By: Angelo Corsaro, CTO, PrismTech - April 28th, 2016

As the Internet of Things (IoT) continues its rapid pace of growth, there's been no shortage of inflated expectations. Platforms promising to ease the development, deployment, and management of IoT systems are now counted in the hundreds. You might be led to believe that all you have to do is pick a platform you like the best, from the vendor you trust the most, and go build your IoT system. Well, the story is not so simple.

In reality, nearly all of the IoT platforms available are designed to only support cloud-centric architectures. These platforms centralize the "intelligence" in the cloud and require data to be conveyed from the edge to do anything useful with it. Considering the success of this cloud-centric model in IT (and in some IoT applications like fleet management), you may wonder—what's the big deal?

Simply put, cloud-centric architectures aren't applicable to a large class of IoT applications. Most notably, cloud-centric architectures fall short in supporting Industrial IoT (IIoT) systems and struggle with more demanding Consumer IoT (CIoT) applications.

The scariest part is that the situation will only get worse with the predicted increase in the number of connected things. But the problem goes beyond the sheer number of things. There's something more fundamental limiting cloud-centric architectures' applicability for IoT systems. Let's go through them one by one.

Cloud-centric architectures assume that sufficient connectivity exists from the things to the cloud. This is necessary for collecting the data from the edge, and for pushing insight or control actions from the cloud to the edge. Yet, connectivity is hard to guarantee for several IoT/IIoT applications, such as smart autonomous consumer and agricultural vehicles. As you can imagine, connectivity may be taken for granted in metropolitan areas, but not so much in rural areas.

Cloud-centric computing assumes that sufficient bandwidth exists to ingest the data from the edge into the data-center. The challenge here is that several IIoT applications produce incredible volumes of data. For instance, a factory can easily produce a 1 Tbytes of data per day. And these numbers will only grow with the continued digitalization of factories.

Let's assume that the connectivity and bandwidth problem is solved. All good now? Nope. There's still a large class of IIoT systems for which the latency required to send data to the cloud, make decisions, and eventually send data toward the edge to act on these decisions may be completely incompatible with the dynamics of the underlying system. A key difference between IT and IoT/IIoT is that the latter deals with physical entities. As such, the reaction time can't be arbitrary; it must be compatible with the dynamics of the physical entity or process with which the application interacts. Failing to react with the proper latency can lead to system instability, infrastructure damage, or even put human operators at risk.

In the age of smartphones and very cheap data plans, most people assume that the cost of connectivity is negligible. The reality is quite different in IIoT due to either bandwidth requirements or connectivity points. While in consumer applications, the individual person—the consumer—pays for connectivity. In most IoT/IIoT applications, such as smart grids, it's the operator who foots the bill. As a result, the cost is usually carefully accounted for as it has an impact on OPEX and consequently on operational costs and margins.

Finally, even assuming that all the above listed issues are addressed, a large class of IIoT applications are not comfortable, or are incapable due to regulations, to push their data to a cloud.

In summary, unless you can guarantee that the connectivity, bandwidth, latency, cost, and security requirements of your application are compatible with a cloud-centric architecture, you need a different paradigm, and 99.9% of the IoT platforms available on the market are not of much use.

Fog computing is emerging as the main paradigm to address the connectivity, bandwidth, latency, cost, and security challenges imposed by cloud-centric architectures. The main idea behind fog computing is to provide elastic compute, storage, and communication close to the things so that data needn't be sent all the way to the cloud, or at least not all data and not all the time. And the infrastructure is designed ground-up to deal with cyber-physical-systems (CPS) as opposed to IT systems. In other words, the infrastructure is designed to consider the constraints imposed by the interactions with the physical world in terms of latency, determinism, load balancing, and fault-tolerance.

Angelo Corsaro, Ph.D., is the Chief Technology Officer at PrismTech, where he directs the company's technology strategy, planning, evolution, and evangelism. He also leads the strategic standardization at the Object Management Group, where he co-chairs the Data Distribution Service Special Interest Group and serves on its Architecture Board. Angelo earned a Ph.D. and a M.S. in Computer Science from the Washington University in St. Louis, and a Laurea Magna cum Laude in Computer Engineering from the University of Catania, Italy.

See the VIDEO: Vortex ADLINK IoT Gateway Demo Click Here

ADLINK IoT Gateway Kit, End-to-End Solution: see page 8

Sierra Wireless enables the world's fastest vehicle network for first responders, field services and transit

AirLink® MP70 Vehicle Router solves challenge of connecting multiple high-bandwidth in-vehicle applications with LTE Advanced, Gigabit Wi-Fi and Gigabit Ethernet connectivity

Vancouver, Canada-May 17, 2016 -- Sierra Wireless (NASDAQ: SWIR) (TSX: SW) today announced availability of the AirLink® MP70, an LTE-Advanced (LTE-A) vehicle router for mission critical applications in public safety, transit and field services. Today's mobile workforce needs to connect more technology in and around their vehicles to enhance safety and responsiveness. The MP70 serves as a purpose-built, high-performance vehicle networking solution that enables multiple high-bandwidth applications to work simultaneously, more than 10 times faster and four times further from the vehicle than ever before. It also provides IT departments with the flexibility to manage fleet and mobile assets in the cloud or in the enterprise data center using Sierra Wireless AirLink Network Management solutions.

“First responders and field services teams need access to uncompromised connectivity at all times, and that's central to all of our LTE networking solutions,” said Jason Krause, Senior Vice President and General Manager, Enterprise Solutions for Sierra Wireless. “Using the MP70, mobile workers can communicate seamlessly from in and around their vehicle, as if they were in an office. This allows them to perform critical duties onsite more efficiently, and ultimately respond more quickly and effectively in the field.”

For example, a typical law enforcement vehicle hosts a laptop for dispatch and records management, an electronic citation system, live digital video surveillance, body-worn cameras and automated license plate recognition (ALPR) systems. With the MP70, all of these systems can connect to a high-speed vehicle area network, with both gigabit Ethernet and 802.11ac Wi-Fi supported, and share a secure LTE-A cellular connection that enables the dispatcher to access all of the systems in real time.

“We trialed the MP70 router to connect our in-vehicle computers and provide a Wi-Fi hotspot for our team to access critical database records onsite in real time during emergencies,” said Greg Katz, Lieutenant, Billerica MA Police Department. “Right out of the box, we were impressed by the MP70's top-notch, ruggedized form factor—with hardened aluminum casing, it's clearly designed for turbulent vehicle environments. We are also very impressed with its reliable LTE connectivity and, because it offers 4-port Gigabit Ethernet, we will be able to support more in-vehicle equipment, such as video cameras and ALPR, bringing the full functionality of our office network to our patrol officers.”

“The MP70 high performance vehicle router extends Sierra Wireless' industry leading portfolio of vehicle gateways, which includes the AirLink GX450 mobile gateway and multi-network FirstNet Band 14 oMG vehicle router,” said Robin Duke-Woolley, CEO of specialist IoT analyst firm Beecham Research. “There is strong demand for vehicle area networks that can handle multiple applications, and the MP70's flexible, secure management and Wi-Fi capabilities make it an attractive option.”

An entire fleet of AirLink MP70 routers, field applications and mobile assets can be remotely managed, controlled and monitored over a centralized platform using AirLink Network Management solutions from Sierra Wireless. Available as a hosted, cloud-based AirLink Management Service, or as a licensed software platform in the enterprise data center, oMM Management System, AirLink Network Management solutions allow organizations to increase efficiency and lower maintenance costs by up to 90 percent.

SIERRA WIRELESS

MORE: Click Here

Our 4 Magazines

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

FREE just Click on the LOGO

IoT World

Telecom COTS World
Broadband Broadcast IoT Convergence

Embedded Systems World

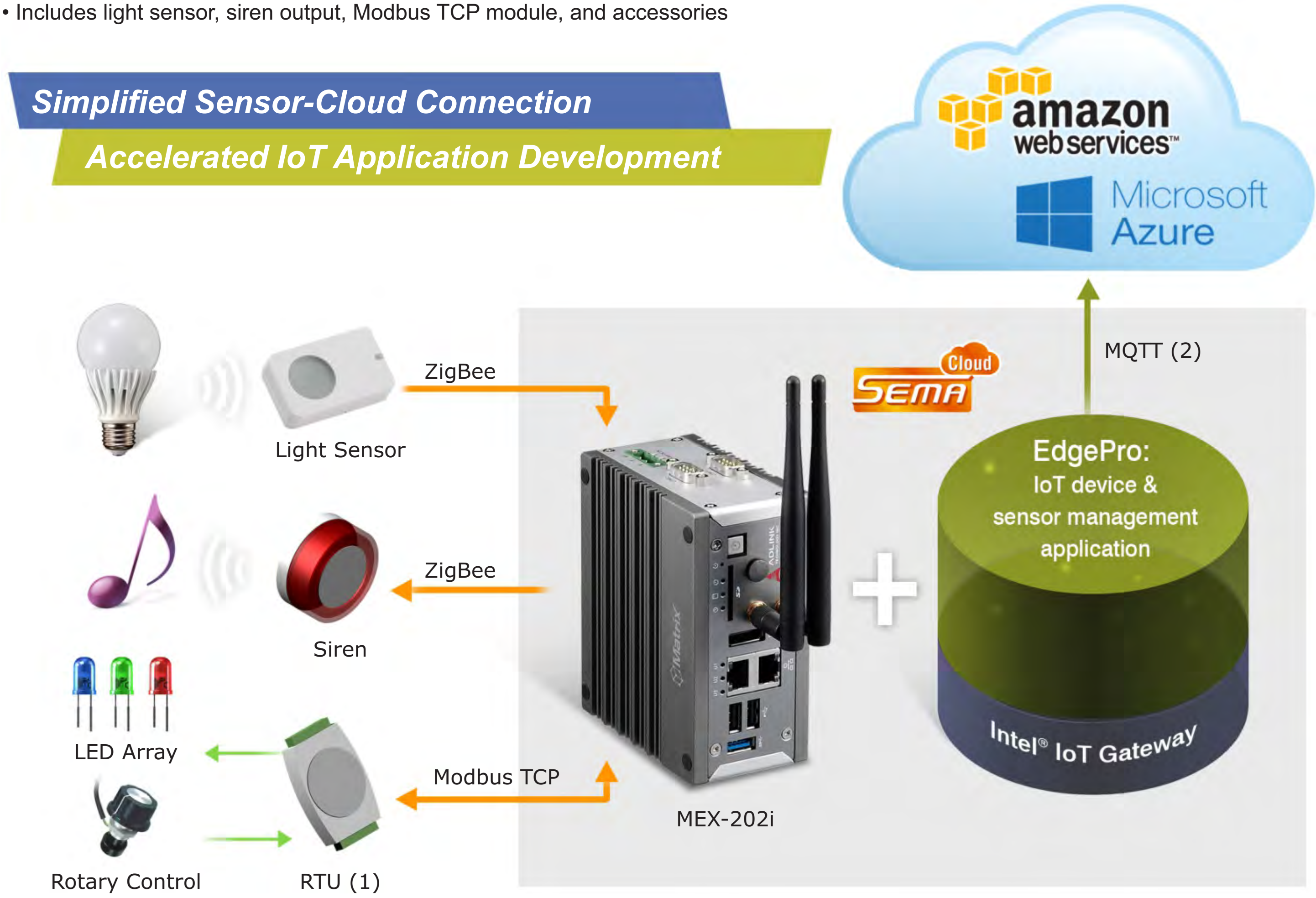
ATCA World

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

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

Features:

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



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

The Intelligent IoT Gateway Starter Kit includes:

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

More:

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

Contact

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

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

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

ADLINK TECHNOLOGY INC.

intel IoT Solutions Alliance Premier