Title*: PoC Proposal: MEC platform to enable low-latency Industrial IoT

from **Source***: Vasona Networks Inc
Contact: Rui Frazao, Ariel Peltz apeltz@vasonanetworks.com

input for **Committee***: MEC

Contribution **For***:

Decision	X
Discussion	
Information	

Submission date*: 2017-01-04

Meeting & Allocation: Relevant WI(s), or deliverable(s):

Decision/action requested: Please approve

ABSTRACT: *This is an MEC PoC submission about MEC Architecture and MEC Service Scenarios focused on Industrial IoT use cases*

PoC Proposal

1 PoC Project Details

1.1 PoC Project

PoC Number (assigned by ETSI):

PoC Project Name: MEC platform to enable low-latency **Industrial IoT (Internet of Things)**

PoC Project Host: **Vasona Networks**

Short Description: *This ETSI MEC and ETSI NFV compliant PoC considers a typical **Industry 4.0 (RAMI 4.0 - Platform 4.0 Industrie)*** IoT use-case for latency, mobility and location sensitive applications, wherein a standards compliant MEC host with local RAN breakout can enable massively scalable real-time duplex trusted transit delivery of data between IoT devices (sensors, actuators, control systems etc.) and cloud based industrial applications that leverage low-latency transactions with real-time meta-data on localized usage, security and QoS. The PoC will simulate a real-world Industry 4.0* use case and demonstrate several value drivers for stakeholders driving IoT.*

This PoC will leverage Xaptum's distributed Peering IP-Overlay Network for IoT and extend their peering Xaptum ENF (Edge Network Fabric) Run-Time Architecture to the mobile edge for low latency and secure communication in Industrial IoT devices and applications. By combining Xaptum ENF with Oberthur's embedded cryptographic authentication SE (Secure Element) offering and vendor neutral TPM 2.0 (Trusted Platform Module) and DAA (Direct Anonymous Attestation) to both IoT device and application end-points, we shall be able to demonstrate several use-cases that meet stringent requirements for industrial applications as defined by leading Industry 4.0 standards.*

The entirety of the PoC will be deployed over an ETSI NFV compliant infrastructure to highlight the benefits of COTS hardware and to reap the benefits of orchestration and automation. The PoC will leverage RIFT.io RIFT.ware, a commercially supported offering of the ETSI Open Source MANO (OSM) group.

(*) http://www.plattform-i40.de/ (Initiative from German Govt. leading the way in Industry 4.0), https://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/rami40-an-introduction.pdf?__blob=publicationFile&v=3

1.2 PoC Team Members

	Organisation name	ISG MEC participant (yes/no)	Contact (Email)	PoC Point of Contact (*)	Role (**)	PoC Components
1	Vasona Networks	Yes	Ariel Peltz apeltz@vasonanetworks.com	X	Infrastructure Provider	Vasona OpenStack based infrastructure and SmartAIR Edge Services Platform
2	RIFT.io	No	Noel Charath Noel.Charath@riftio.com		Infrastructure Provider	RIFT.ware ETSI compliant Open Source MANO platform
3	Xaptum	No	Pradeep Barthur Pradeep@xaptum.com		Application Provider	(i) Multi-radio GPIO Edge Gateway's & (ii) Edge Computing SD-WAN IP-Overlay Network
4	Oberthur Technologies	No	Stephane Andrau S.ANDRAU@oberthur.com		Application Provider	eSE/TPM 2.0 HSM for eSE
5	Intel Corporation	Yes	Anil Keshavamurthy Anil.s.keshavamurthy@intel.com		Infrastructure Provider	IoT Edge Gateway Platform (H/W & S/W components)
6	Vodafone	Yes	Guenter Klas Guenter.Klas@vodafone.com		Service Provider	Guidance and feedback from Operator

(*) Identify the PoC Point of Contact with an X.
(**) The Role will be network operator/service provider, infrastructure provider, application provider or other.

All the PoC Team members listed above declare that the information in this proposal is conformant to their plans at this date and commit to inform ETSI timely in case of changes in the PoC Team, scope or timeline.

1.3 PoC Project Scope

1.3.1 PoC Topics

PoC Topics identified in this clause need to be taken from the PoC Topic List identified by ISG MEC and publicly available in the MEC WIKI. PoC Teams addressing these topics commit to submit the expected contributions in a timely manner.

PoC Topic Code	PoC Topic Description	Related WG/WI	Expected Contribution	Target Date

PT01	Demonstration of MEC Service Scenarios	MEC-004 Service Scenarios
		
		MEC-009 General Principles for Mobile Edge Service APIs
			PC1 - Technical report and demonstration with the following lessons learned and technical information:
			• MEC Services (Vasona instance):
			  ○ IoT traffic detection
			  ○ Dynamic local breakout of IoT traffic
			• MEC Application (Xaptum instance):
			  ○ IoT edge platform with secure connection to industrial gateway
				Mobile World Congress March 2017

PT03	MEC Architecture	MEC-006 - Metrics Best Practice and Guidelines MEC-010-1 System, Host, and Platform Management	PC1 - Technical report and demonstration with the following lessons learned and technical information: • Demonstrate MEC Server architecture based on COTS,	MEC Congress September 2017

		MEC-010-2 Application Lifecycle, Rules, and Requirements Management MEC-011 Mobile Edge Platform Application Enablement MEC—017 Deployment of Mobile Edge Computing in a NFV Environment	OpenStack and OpenSource MANO • Demonstration of MEC NFV-I and Cloud Orchestration supporting dynamic instantiation of IoT gateway and local breakout network rules • Integration of MEC NFV-I into mobile network (local breakout) • Report application latency as measured by ME Platform	

1.3.2 Other topics in scope

List here any additional topic for which the PoC plans to provide input/feedback to the ISG MEC.

PoC Topic Code	PoC Topic Description	Related WG/WI	Expected Contribution	Target Date
A				
B				
<…>				

1.4 PoC Project Milestones

PoC Milestone	Milestone description	Target Date	Additional Info
P.S	PoC Project Start	Jan 1, 2017	
P.D1	PoC Demo 1 – Static setup of local IoT traffic breakout	Feb 2017	Mobile World Congress 2017, Barcelona
P.D2	Poc Demo 2 – Dynamic setup of local IoT traffic breakout based on performance KPIs or external trigger	Sep 2017	MEC Congress 2017, Berlin
P.C1	PoC Expected Contribution 1	Q3 2017	Publish APIs used in the PoC
P.R	PoC Report	Q4 2017	Publish a final report for the PoC
P.E	PoC Project End	Dec 2017	

NOTE: Milestones need to be entered in chronological order.

1.5 Additional Details

For example, URL, planned publications, conferences, etc.

2 PoC Technical Details

2.1 PoC Overview

Mobile Edge Computing (MEC) provides a new ecosystem and value chain, and the opportunity for new players to collaborate and develop new business models they can each benefit from. This PoC will focus on bringing together the MEC capabilities with a specific Internet of Things (IoT) industrial use case and associated communication and security standards.

In this PoC we will focus on building a vertical solution that addresses today's requirements of industrial customers and demonstrates the feasibility of building a new service model within the mobile infrastructure by combining the following value drivers:

- **Mobile Low Latency traffic management: Policy-driven Traffic Detection, Breakout and Advanced Session Mapping on a Mobile edge platform :** Vasona provides RAN I/O breakout using IoT traffic detection for (i) Responsive Routing (computing resources generating and consuming data packets in different namespace): between multiple clouds (like AWS, Azure etc.) hosting IoT applications and IoT devices and (ii) Synchronization Routing (computing resources generating and consuming data packets in same namespace): between multiple intelligent IoT devices that can also host applications, detects traffic patterns based on traffic policy and maintains PGW session status towards mobile core.

- **Scalable IoT Device and Application Endpoint Security: Digital Anonymous Attestation (DAA), Embedded Hardware Cryptography with HSM/SSM (Hardware Security Module/Software Security Module)-DAA Validation by Oberthur Technologieswith Xaptum ENF:** While enabling massive dynamic duplex multiplexing of IoT traffic, implementing Xaptum ENF eliminates the need for a static PSK (Pre-Shared Encryption Key). Using Elliptic Curve Cryptography (ECC) with DAA, the IoT device and Xaptum ENF can generate an ephemeral PSK to establish an encrypted TLS (Transport Layer Security) based session.

- **Trusted Transaction Model: Trust Transit Access, Trusted Transit Security and Advanced Routing by Xaptum:** Xaptum's distributed Peering IP-Overlay Network enables massive dynamic duplex multiplexing of IoT traffic with security, AAA, QoS and dynamic routing policies with the Publishers (PUB)/Sub (Subscribers) of IoT data packets, whether IoT device or application end-points are now hosted at the mobile edge, closer to the RAN. This trusted transaction model will ensure transparency on optimization of bandwidth and radio resources with low-latency, QoS based packet delivery that include robust secure transaction model.

Edge Gateways simulating Industrial IoT data: We will simulate two Industrial factories sending IoT data to cloud and to other factory and demonstrate low latency communication among them achieved through services running on ME Platform.

The ME Platform will track and report latency (RTT) of IoT traffic both for cloud communication and local breakout communication, demonstrating the ability to ensure low-latency for inter-factory communication. The Xaptum ME App will report on latency of IoT messages crossing the platform.

2.2 PoC Architecture

This PoC will be built around the premise of connecting two Industrial Factories within a region served by a mobile network where full duplex, secure and low latency messages need to be exchanged between the two locations (see figure 1 below).

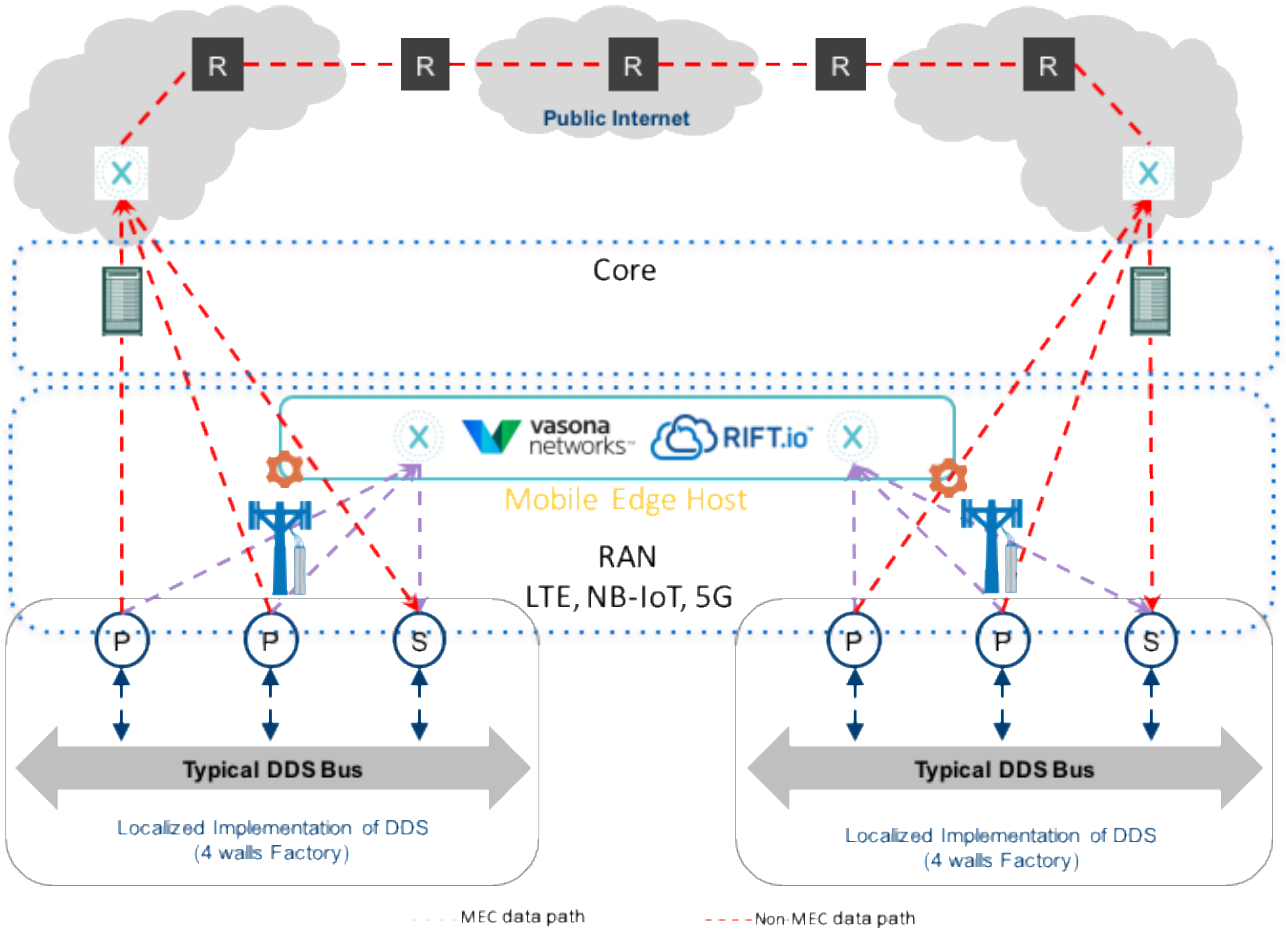

Figure 1- Illustration of PoC Test Bed

In order to realize this solution, we will use a generic NFV Infrastructure based on interchangeable COTS and Open Source elements: OpenStack, MANO and vSwitch. The ME platform functions will be performed by Vasona's Edge Service Platform which will be inserted in-line between the RAN and the Core of the mobile network. Both the RAN and the Core will be emulated and run on separate Virtual Machines (external to the ME Host). The end-user devices will be "factory controllers" running Xaptum's GUI test emulator exercising different test cases.

The factory controllers are Dell Edge Gateway 5000 Series based on Intel's reference architecture. They can be used both as an emulator or connect to factory's actuator controllers or DC system. In this specific testbed, we will use two controllers placed in two different factory locations (different cell sites) and use a mix of emulated messages and proximity sensors that need to be acknowledge by the remote location.

The Xaptum Edge Network function will be deployed on a VM as a Mobile Edge Application and will be responsible for authentication, encryption and routing of the IoT messages both within the RAN environment and to the cloud through a secure internet connection.

Management and Orchestration (MANO) of the various Virtual Network Functions (VNF) will be performed by RIFT.io RIFT.ware, which performs the network service orchestration and Network Service and VNF lifecycle management functions (onboarding, catalogue management, instantiation, and termination) for all virtual components.

The Vasona Edge Services Platform (ME Host and ME platform functions) will, based on pre-established IoT destinations, or through external request from Xaptum's IoT clients, breakout traffic to the hosted Xaptum ME App, whilst maintaining GTP integrity.

A dashboard on the Xaptum ME App will report the KPIs for both local breakout routed and internet routed messages, demonstrating compliance with the low latency requirements. A proximity sensor with a visual element (LED based) will be added to the factory controllers to demonstrate when the communication between the two factory locations is within the latency requirements.
The ME Platform will track and report IoT traffic latency demonstrating difference between local breakout and cloud routed messages.

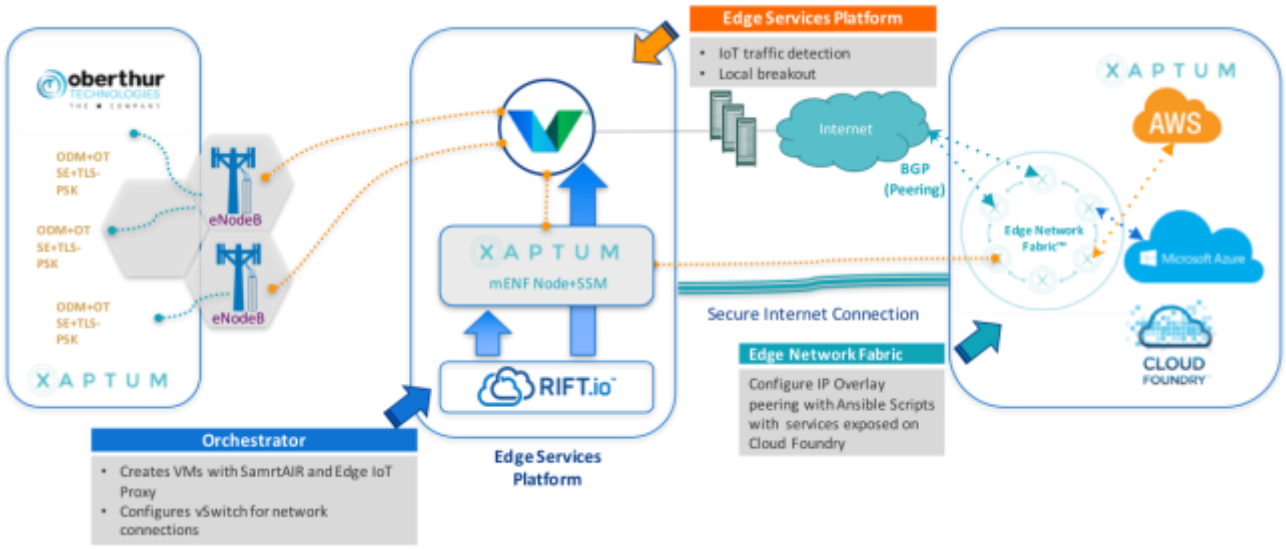

Figure 2- Illustration of End-to-End PoC Architecture

Architecturally, the solution above maps to the ETSI MEC ISG architecture defined in **Mobile Edge Computing (MEC); Framework and Reference Architecture** (ETSI GS MEC 003 V1.1.1), as follows.

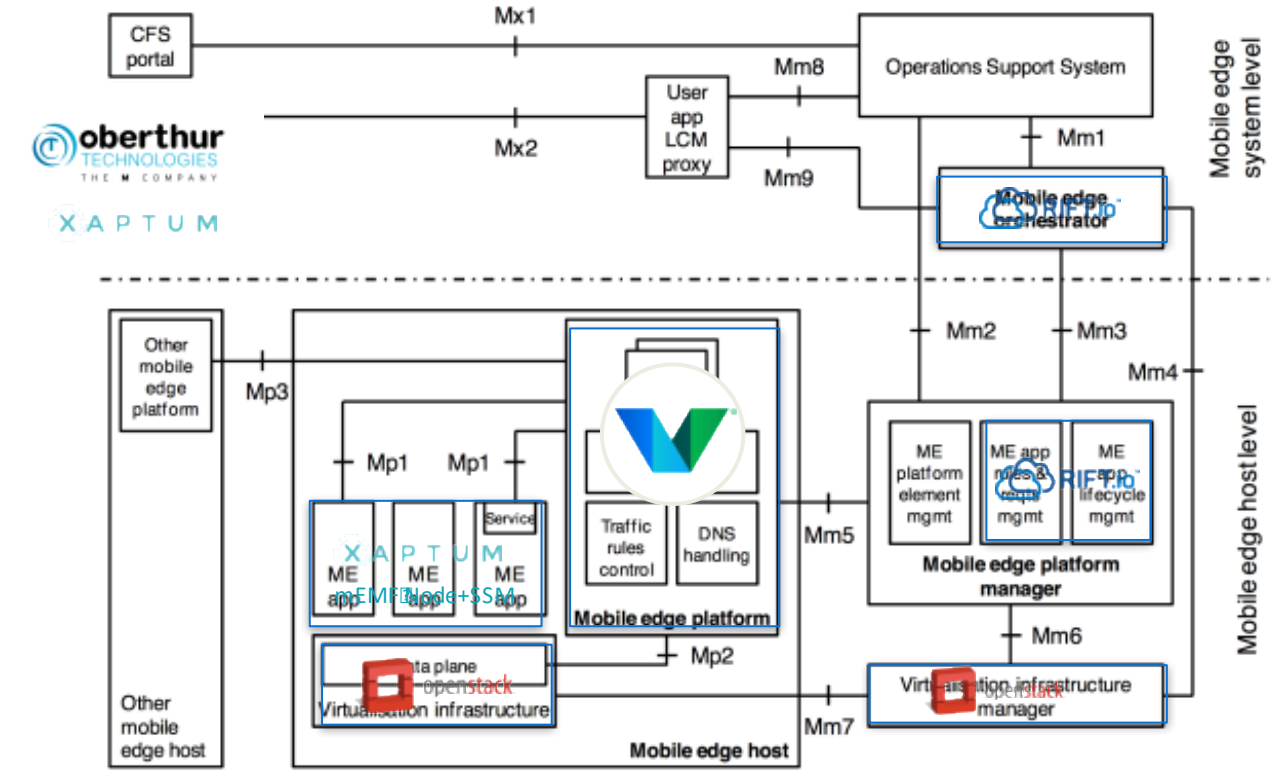

Figure 3- Mapping of MEC PoC with ETSI GS MEC 003 V1.1.1 Reference Architecture

2.3 Additional information

2.3.1 Security Model Reference Architecture by Oberthur Technologies

Schematic architecture of Embedded Hardware Cryptography with HSM (Hardware Security Module/Software Security Module service model-\ with DAA Validation by Oberthur Technologies with Xaptum ENF, is shown below in figure 4 and its interaction with the ETSI ME Host.

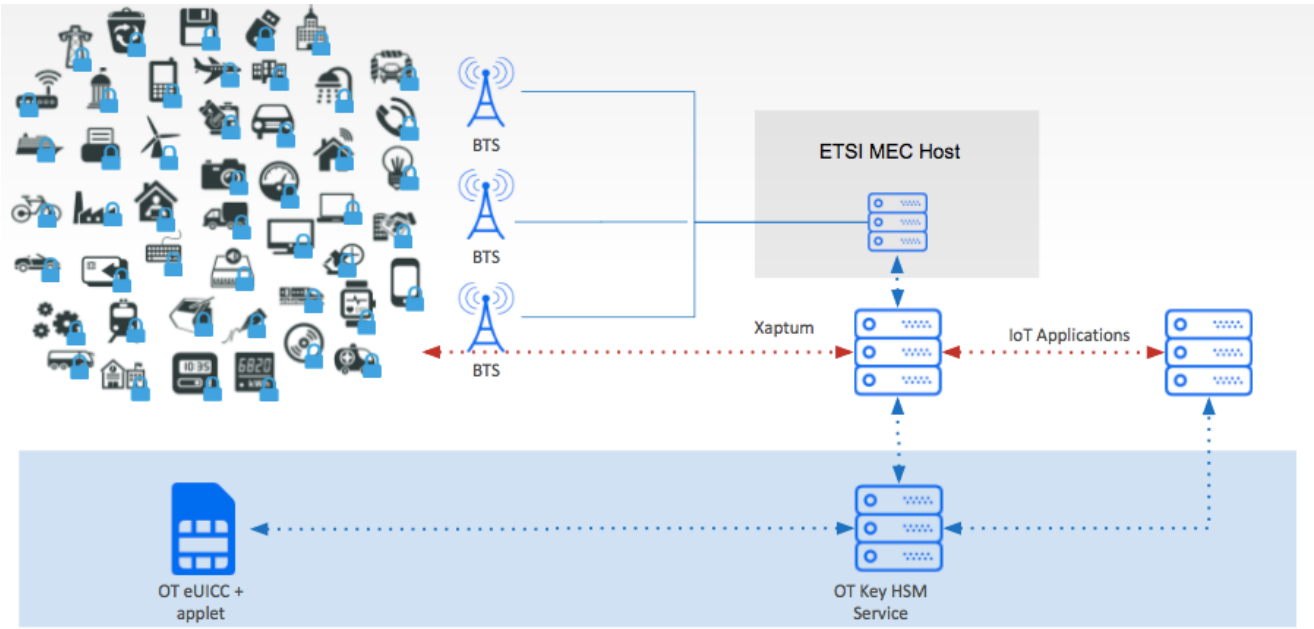

Figure 4- Illustration Interaction Schematic of Security Model enabled by Oberthur Technologies

2.3.2 Edge Gateway Reference Architecture by Intel Corporation

Schematic architecture of Edge Gateway in Industry 4.0 PoC, Intel has provided Falcon Beach Reference Architecture for Edge Gateways that is being used by ODMs to build edge gateway's including for the PoC. This gateway is based on Intel Atom E3805, has two cores running at 1.33GHz supporting 1067MHz DDR3 memory.
Security will be a key differentiator with Intel Gateway supporting variety of security technologies including EPID, secure boot with hardware root of trust, etc. On the manageability side we will include Wind River Helix Cloud as our gateway manageability solutions.

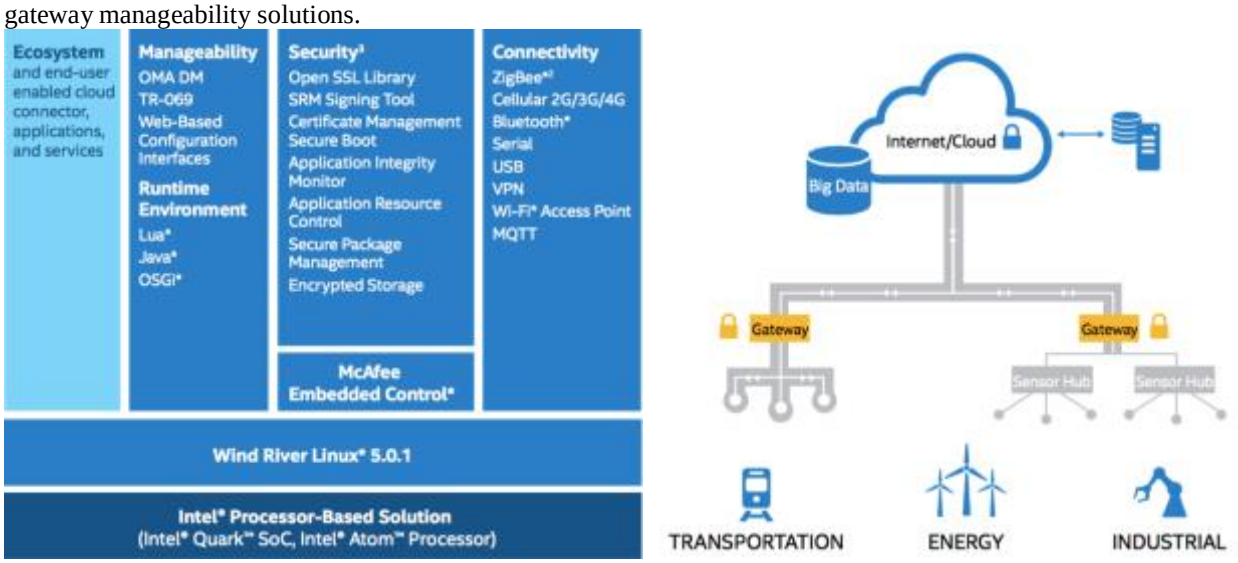

Figure 5- Edge Gateway Stack and Use Case Illustration, based on Intel's Falcon beach Reference Architecture