OpenFog Consortium

Introduction and Overview at W3C Open Day

May 2017

Agenda

- What’s Fog Computing?
- OpenFog Consortium
- OpenFog Reference Architecture
- Technical WG Focuses (Security, Smart Objects, Manageability)
- Moving Forward..
- Q&A

What’s Fog Computing?

What is fog computing?

System-Level

from Things to the Edge, and over the Core to the Cloud, spanning multiple protocol layers

(works over and inside wireless and wireline networks)

Architecture

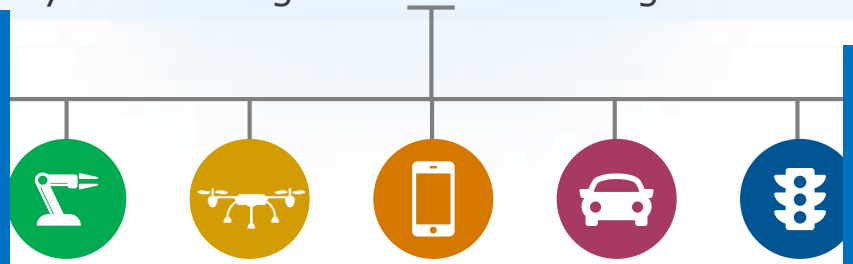
for distributing, orchestrating, managing, securing resources and services

(not just placing servers, computing resources, apps, or small clouds at the edges)

CLOUD

FOG COMPUTING

A system-level horizontal architecture that distributes computing, storage, and networking closer to users, and anywhere along the Cloud-to-Thing continuum



Horizontal

Supports multiple industries

(not limited to any specific industry, network type, or application domain)

Cloud-to-Thing Continuum

Distributes resources and services to anywhere along the continuum

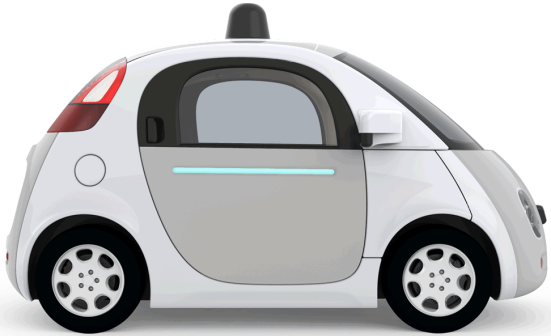
(not just at the edges)

Converged Cloud/Fog platforms and services

(not just isolated edge computing devices / apps)

OpenFog

Why Fog?
It's necessary to run IoT, 5G and AI applications



Selected fog scenarios

Use Cases	1  Traffic Congestion	2  Video Surveillance	3  Smart Buildings
? Problem	$160B cost of traffic delays in US alone	Cloud doesn't scale to support wide-scale surveillance (highways, cities, airports, etc.); rapid security decisions must be made on location	Safety, security, energy efficiency and comfort in buildings is an ongoing concern
⚠ Challenges	Solutions developed in silos hinder information sharing; data sources are bandwidth intensive and complex	HD cameras generate terabytes of data per day	Telemetry data is sent from thousands of sensors simultaneously
Fog Technology	Fog computing ensures sharing of data from vehicles and along roadways	Fog nodes intelligently partition video processing between cameras and cloud, enabling real-time, latency sensitive analytics	Fog computing creates smart, connected spaces; fog nodes for individual rooms can perform all monitoring and response functions

Why fog? Beyond necessary, it enables growth through new business models

Reshape the Industry Landscape

Routers, switches, application servers, and storage servers converge into unified fog nodes

Create Disruptive New Service Models

Players of all sizes, not just massive cloud operators, build/operate fogs and offer fog services → "WiFi Model" and the rise of local/regional fog eco-systems and operators?

Integrate and Converge Cloud–Fog Services

For a business to function as a cohesive whole, cloud and fog will converge into one common infrastructure for integrated and unified cloud and fog services: development, deployment, monitoring, management, security, …

Enable Rapid Development and Deployment of Fog Systems and Applications

Rapid deployment of localized applications → shifting from "build the cloud and see what services we can put on it" to "find what customers want and quickly put together a fog for them"

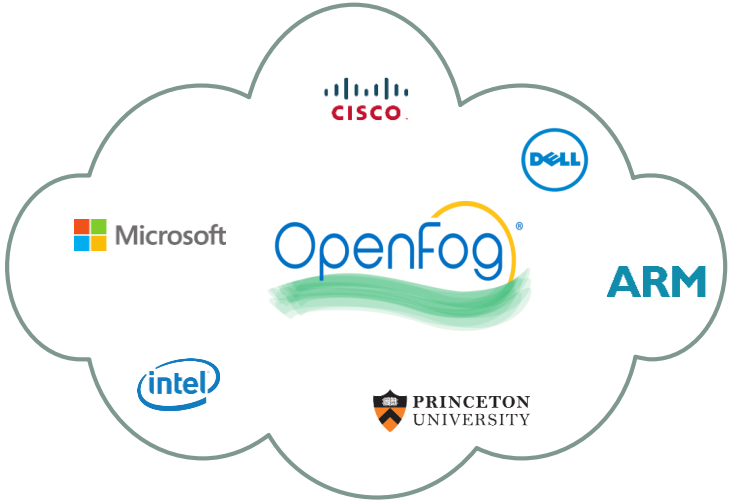
OpenFog

To work, fog computing must have universal interoperability

TCP/IP	WWW	Fog Computing and OpenFog Consortium
A standard and universal framework to distribute packets	A standard and universal framework to access files anywhere	A standard and universal framework to distribute resources and services and Manage, pool, orchestrate, and secure these distributed resources and services
Was it necessary to create a TCP/IP-for-wireless telecom? a TCP/IP-for-wired? a TCP/IP-for-enterprise? … ***NO***	Was it necessary to develop a HTTP-for-wireless? a HTTP-for-wired? a HTTP-for-enterprise? … ***NO***	Is it necessary to develop a fog-like system for 5G? another for wired telecom? another for enterprises? another for smart city? another for manufacturing? … ***NO***

OpenFog Consortium

Building this necessary interoperability of fog-enabled applications requires a collaborative approach



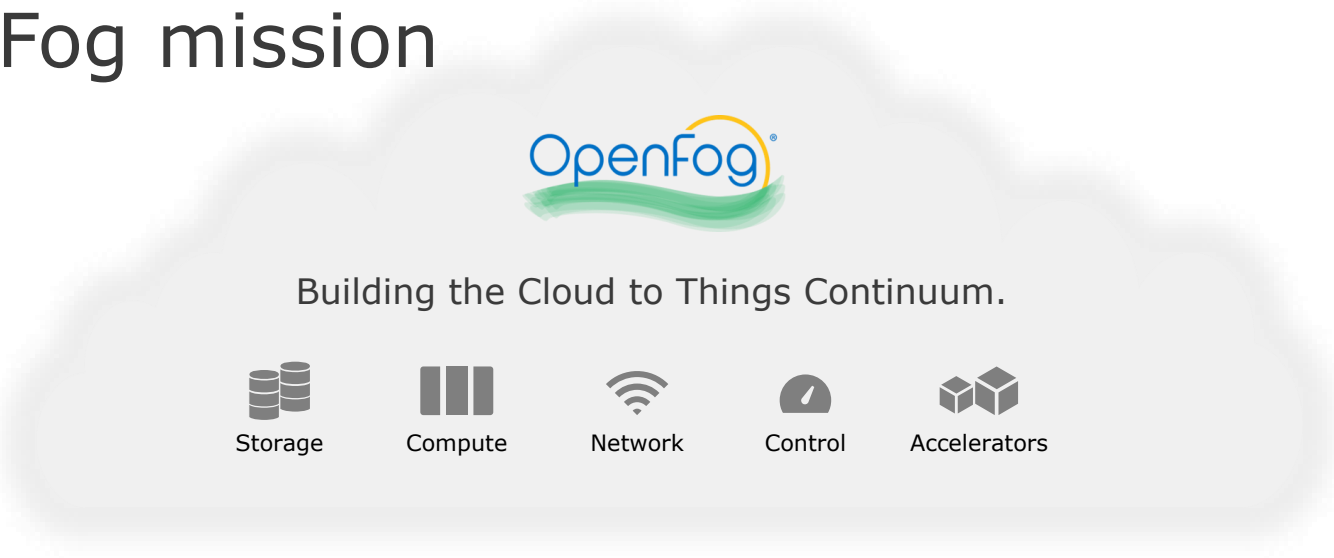
Proprietary or single vendor solutions **slows down** adoption and innovation.

An open architecture will:

- Provide a robust new platform for product development
- Increased quality and innovation through competition in the open environment
- Lead to a vibrant, growing supplier ecosystem
- Accelerate market adoption
- Lower system costs

OpenFog

OpenFog mission



Mission Statement: To drive industry and academic leadership in **fog computing architecture**, testbed development, and a variety of **interoperability** and **composability** deliverables that seamlessly leverage cloud and edge architectures to **enable end-to-end IoT** scenarios.

OpenFog Consortium

A growing, global ecosystem of fog experts

Affiliations

Barcelona Supercomputing Center (Centro Nacional de Supercomputación)
IEEE ComSoc (IEEE Communications Society)
IoT Acceleration Consortium

Founders

ARM
Dell
Microsoft
Cisco
Intel
Princeton University

Contributing Members

AT&T
Foxconn
Sakura internet
GE
Hitachi
Shanghaitech University
ZTE

Fujitsu
Foghorn
Sensify
Toshiba
nebbiolo technologies
Schneider Electric
imec
California Institute of Technology
TTTech
Seagate
Vanderbilt University
P/A
DenverSouth
Singapore University of Technology and Design
Università di Pisa
Kii
CTC
Challenging Tomorrow's Changes
Boulder
Technische Universität Dresden
Prismtech
rti
LGS Innovations
Anjie Services
NGD systems
Bringing Intelligence to Storage
USC
Institute for Information Industry
MARSEC
ASU
The University of Georgia
OSIsoft
National Taiwan University
NEC
relayr.
SRC
Redefining possible
ABBALab
Mitsubishi Electric
IIJ
Internet Initiative Japan
NTT Communications
Aalto University
National Chiao Tung University
Wayne State
ITRI
Industrial Technology Research Institute
Incheon National University
AetherWorks

57 members strong, headquartered in 15 countries as of May 2017

OpenFog Consortium goals

Technology

Develop, Solve, Identify & Create

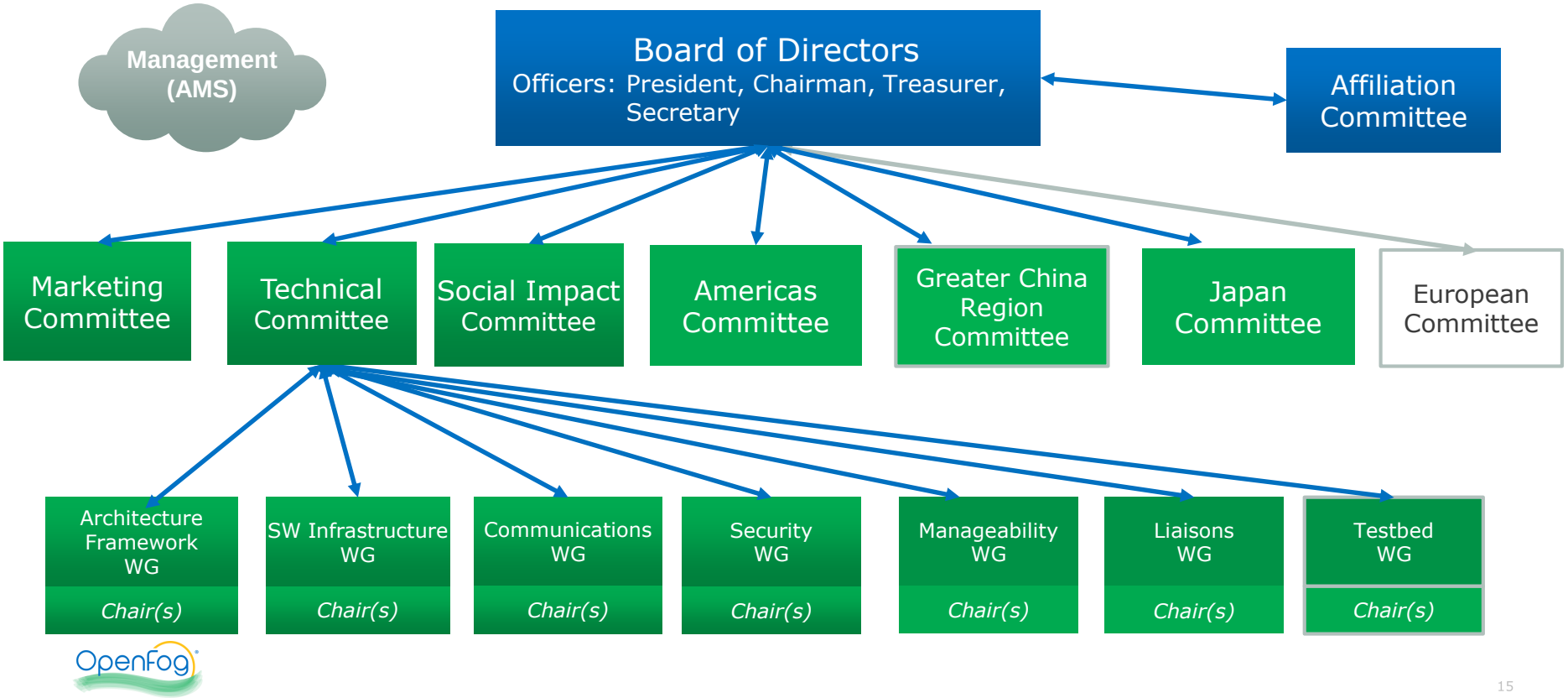
Innovation

Foster, Initiate, Provide & Influence

Education

Gain, Promote, Evangelize & Educate

Organizational structure



Japan Region Committee

Alt. Voice of the Regional Committee
Conduit to BoD

Deputy Liaison

OpenFog — Jeff Fedders

Host/Fund Operational Model Assist Initiatives

Tech-Seat

CISCO — Imai Toshihiro

Voice of the Regional Committee Leads Committee Meetings
Co-Conduit to BoD

R-Director Chair

HITACHI Inspire the Next — Makoto Yasuda

Host/Fund Operational Model Assist Initiatives

Tech-Seat

intel — Masahiro Shimohori

Lead technical agenda Incl. collaboration with global team

Tech-Leads

- Architecture Framework Leads
- SW Infrastructure Leads
- Communication Leads
- Security Leads
- Manageability Leads
- Testbed Champ

Japan Regional Committee

Japan IoT R&D, Standards, Ventures and Policies

Local Consortia

IoT Acceleration Consortium

Tech Liaison-Seat

Liaison to Regional Standards Bodies

ABBALab — Niki Agata

Marketing-Seat

Orchestrates Marketing Activities

Government-Seat

Host Annual Fog Event
Conduit to Local Governments
Conduit to Global Initiatives / Activities

Academic-Seat

Represents Academic / University / Research Projects

SAKURA Internet — Osamu Ogasahara

Innovators-Seat

Represents Innovators / Makers

OpenFog

Japan Country Team: Priority Focus Areas

- Focused use cases of regional interest
  - Car Share
  - Connected Smart Factory
- Affiliation with IoT Acceleration Consortium (more than 28,00 members) backed by METI and MIC
- Works in alignment to the OpenFog global Testbed Workgroup & Technical Committee

OpenFog

IoT Acceleration Consortium

OpenFog Reference Architecture

www.OpenFogConsortium.org/RA

The OpenFog Reference Architecture Framework

1. Unified framework & roadmap to help software developers and system architects create the first generation of open fog computing systems develop compute, network, storage and control technologies for the cloud-to-things continuum.

2. First step in creating standards to enable interoperability in IoT, 5G, Artificial Intelligence and other complex data and network intensive applications.

3. Creates a common language for fog computing and will help unify the edge/fog ecosystem under a single, interoperable, testable set of hardware and software standards.

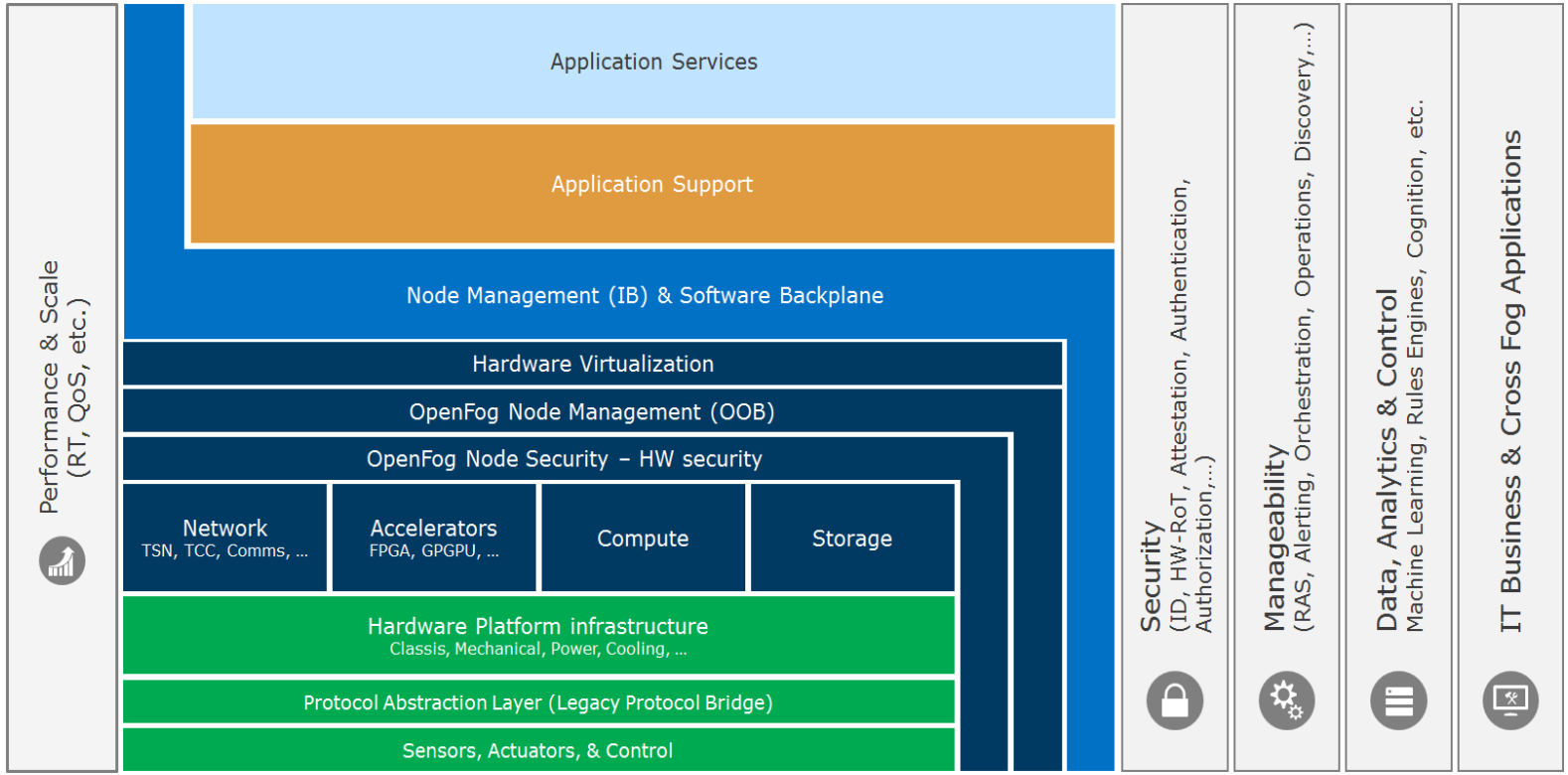
OpenFog

Key pillars of the OpenFog architecture framework

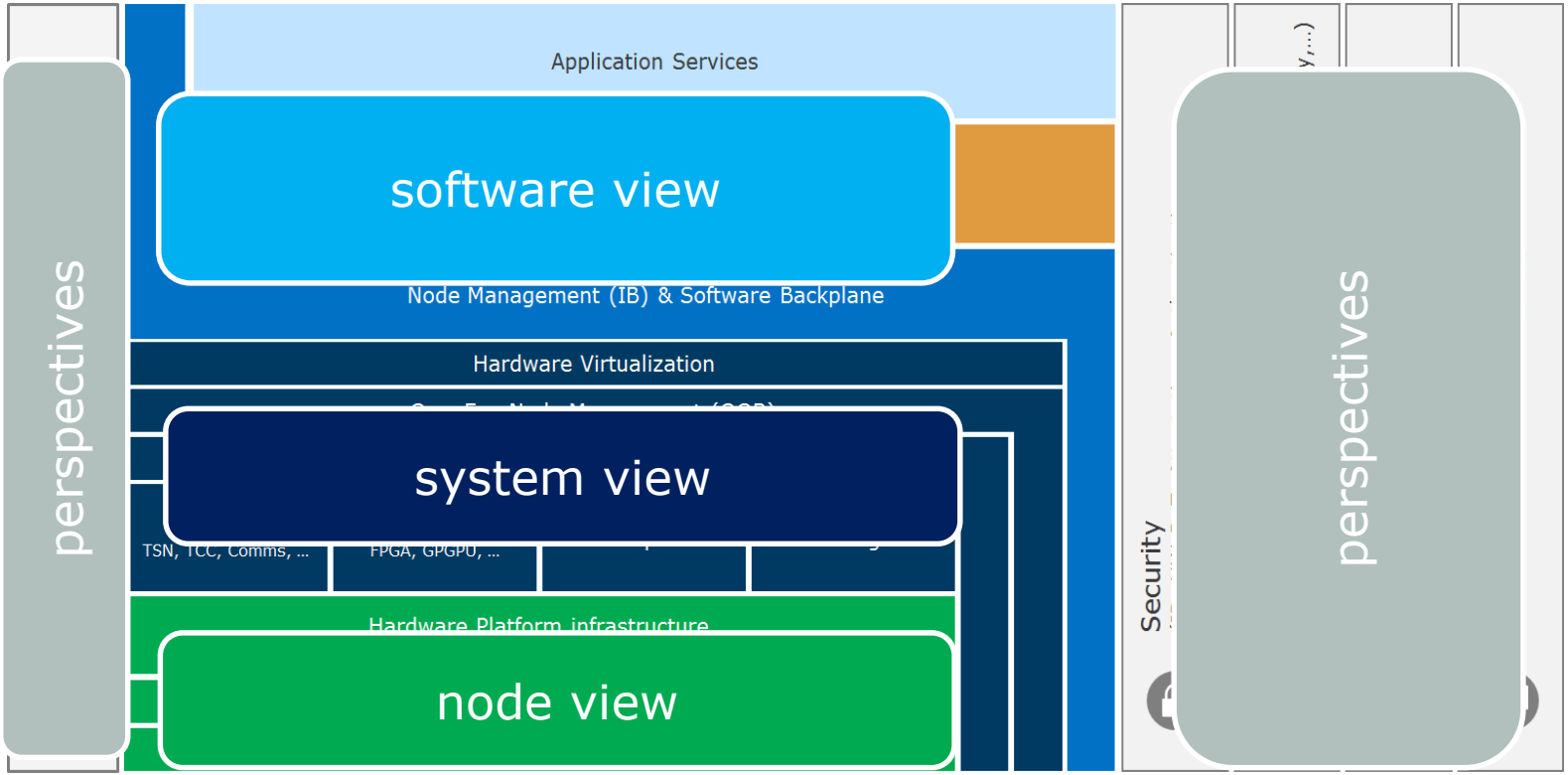
The pillars describe requirements to every part of the fog supply chain: component manufacturers, system vendors, software providers, application developers.

Security	Scalability	Open	Autonomy	RAS	Agility	Hierarchy	Programmability
• Trust • Attestation • Privacy	• Localized command, control & processing • Orchestration & Analytics • Avoidance of network taxes	• Resource visibility & control • White box decision making • Interop & Data normalization	• Flexible • Cognition & agility • Value of data	• Reliability • Availability • Serviceability	• Tactical & strategic decision making • Data to wisdom	• Fully cloud enabled • Computational & System • Autonomy at all levels	• Programmable SW/HW • Virtualization & multi-tenant • App Fluidity

Architecture description with perspectives

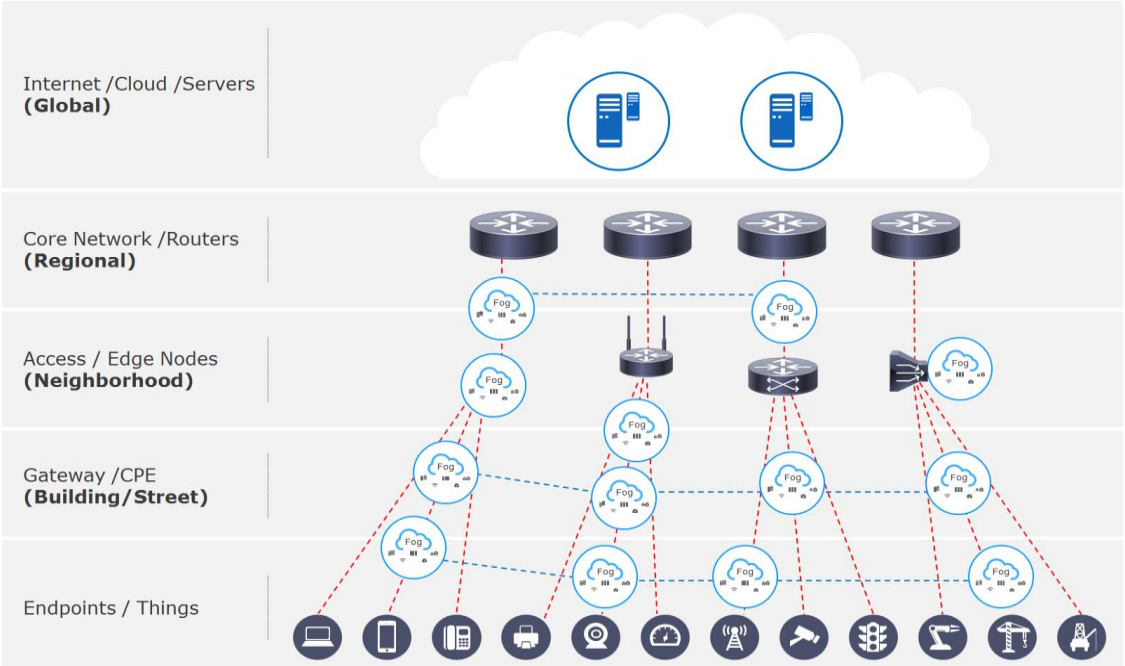


Architecture description with perspectives



A closer look at fog nodes

- They form a mesh to provide load balancing, resilience, fault tolerance, and minimization of cloud communication.
- They communicate laterally (peer to peer, east to west) **and** communicate up and down (north to south)
- Are able to discover, trust, and utilize the services of another node in order to sustain reliability-availability-serviceability



Fog nodes in a Smart City: Buildings, neighborhoods & regions are connected to provide an infrastructure that may be optimized for service delivery.

Technical WG focuses

Security, Smart Objects and Manageability

Security Workgroup

Overview

Reference Architecture Contributions

Node Security

- Node Security is the basis of Fog Security
  - A Hardware Root-of-Trust is the foundation
  - Physical Security needs to be considered for all deployments
- Trusted hardware executes immutable trusted firmware
- Extends the Chain-of-Trust through instantiation of components

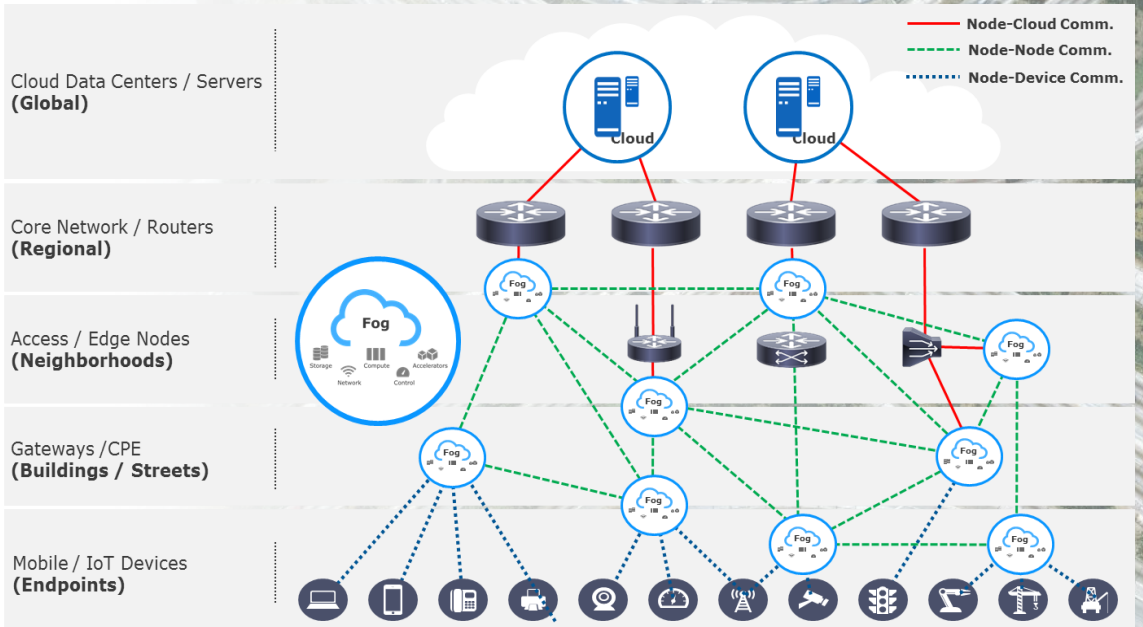
Network Security Aspect

Communications Security

- All communications run through TCP/UDP/IP stack
- Node-to-Cloud
  - WS* / REST over TLS
- Node-to-Node
  - HTTP over TLS
  - COAP over DTLS
- Node-to-Device
  - IP Adaptation
    - WLAN/WPAN: 6LowPAN
    - PLC: PRIME IPv6 SSCS
    - Automation: CIP EtherNet/IP

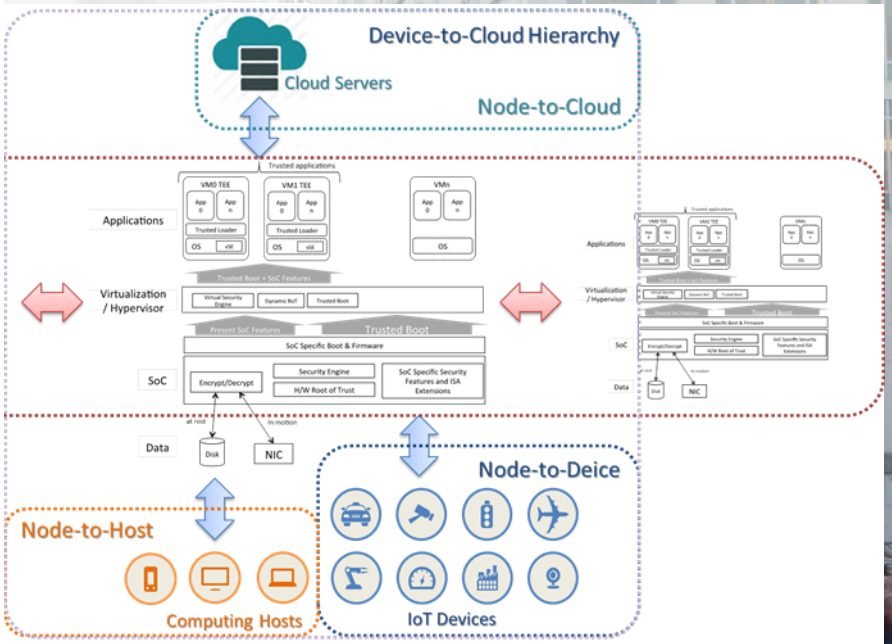
Services Security

- NFV Security Appliances
- SDN Service Provisioning



Data Security Aspect

- **Data in Use**
  - Data in memory undergoing processing
    - Encrypted Memory
- **Data at Rest**
  - Data in storage
    - Full Disk Encryption
    - File / Database Protection
- **Data in Motion/Transit**
  - Data exchanged via (virtual) interfaces
    - Communication Security
    - Content Security



Cryptographic Functions

- A Base Set of Standardized Crypto Functions must be supported by all Fog Nodes to ensure interoperability.
  - An initial base list was selected from FIPS 140-2 spec.;
  - A complete list including regional standardized functions from Europe, China, Japan, … will soon be created.
- Based Set must be updated regularly.
  - NIST Recommendation for Transitioning the Use of Crypto Algorithms and Key Lengths will be followed;
  - Subsequent revision will include transition approaches work for regional crypto functions.
- Compliance does not guarantee security!
  - Crypto Functions selected for fog components should be appropriate for their use and in agreement with stakeholder's threat assessment.
- Formal Validation of Crypto Modules is left as an option to vendors.

New Work & Taskforces

Security Requirement Taskforce

Mission statement

The **mission** of the Security Requirement TF is to define **sets of requirements** that has to express the fundamental security (and in the future evaluation) requirements for an **OpenFog compliant** (in the future certified) node and system.
As a reminder, this work shall support both brown and green field implementations.

The requirements will be split into **3 sets**, each one covering a specific domain of the OpenFog architecture:

- Node Security
- Network/Communication* Security
- Service Management

Strategy

The strategy is define on a **2 phases** basis.

1. **Compliancy program**: In a first phase, the group will focus on the delivery of an OF security compliancy program. A security compliancy program consists of guidelines on security functional requirements for an OF node and system to promote a good level of security.

2. **Certification program**: In its second phase, the group will then focus on delivering a certification program. A certification program consists of precise security functional and evaluation requirements for an OF node and system to assure a measurable level of insurance of security.

* We refer to a network of virtual or physical entities within the Fog.

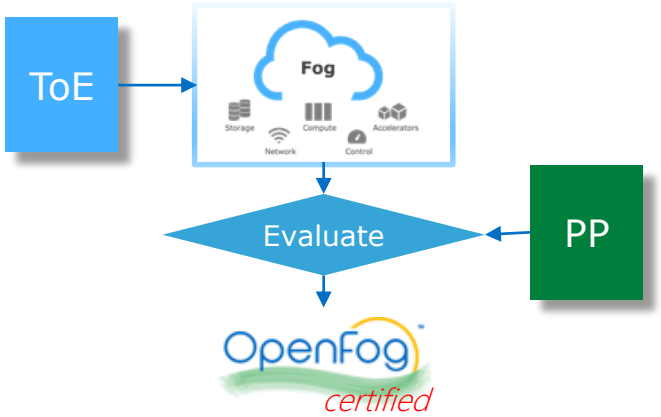
Security Requirement Taskforce

Method

As the plan is eventually to obtain a **certification program** in place, the compliancy phase methodology shall be delivering content that will fully **compatible** for the certification phase.

The **Common Criteria methodology** has been identified as a viable method to build a **Security Certification**. Thus the following CC compatible documents will be produced in the 1st phase for each OF domain listed previously:

- **TOE: Target of evaluation**, defining the product or system that is the subject of the evaluation
- **PP: Protection Profile**, defining the following Security points:
  - Problem definition (Threats, assumption, …)
  - Objectives (ex. protected storage, comm …)
  - Functional Requirements (protecting the TOE in the context of the Problem definition to ensure Objectives)



Deliveries and reporting

The deliveries of the group are **defined by the methodology** and so consist of:

- **TOE** for the 3 domains
- **PP** for the 3 domains
- **Planning** for the Sec WG

* Dependent on reference architecture formal definition progress.

Security MVIs

- Security MVIs
  - Must be described in such that they allow for both innovation and diversity in the solutions provided by different vendors and products, both now and in the future.
  - The MVIs will trace the Security MVIs from power-on until the full system is instantiated.
- A Functional Description of Security MVIs is required
  - Requires a description of how the other system components utilize them.
  - The functional requirements need to be expressed in such a way that they are testable.
- OpenFog systems
  - The components chosen must interoperate with the rest of Fog Computing infrastructure.
- Security MVIs
  - First pass: Will describe the hardware features minimally needed in order to provide a secure base for fog nodes.
  - The Second pass: will define Security MVIs in terms of functions/services from a software perspective

Smart Objects for an OpenFog Architecture:
SW Infrastructure WG – Task Group

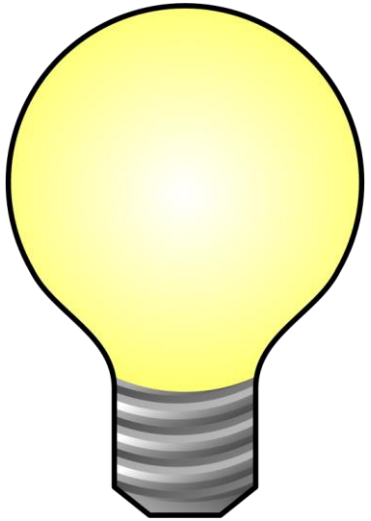
Jeff Sedayao, Eve M. Schooler
Intel IoTG
May, 2017

Smart Objects for an OpenFog Architecture
SW Infrastructure WG – Task Group

- What are Smart Objects?
- Why do we care about Smart Objects?
- Smart Object Landscape
- Smart Object Issues
- Task Group Charter

What's a Smart Object?

- Smart Object: An object that describes its own possible interactions [1]
  - Objects can be **physical**, *e.g.,* sensor, computing device, wearables
  - Objects can be **cyber**, *e.g.,* data, executable code, apps, services, clouds
- A Smart object's description and metadata need to be stored and maintained somewhere
- A Smart Object Framework includes ways to describe, identify, and interact with smart objects



Q. How do you turn on a light bulb?
A. Get a description of how to interact with the light bulb and then turn it on in accordance with the description

Why do we care about Smart Objects?

- Without some form of self-description, IoT object interaction must be built into application logic
  - Code must be added for new object types
  - A problem that really exists [2]
- A Smart object approach promises a way to quickly build and maintain applications
- Commonly cited needs:
  - Data interoperability
  - Service, object, and SW composition

You shouldn't have to hardcode the logic of turning on each different kind of light bulb or each different light bulb vendor

Reduce time and cost to develop, deploy, and maintain IoT applications

Smart Object Landscape

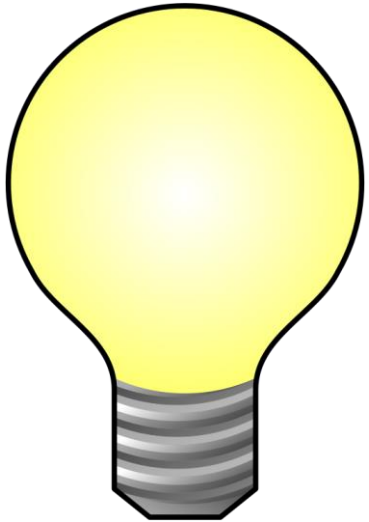
- Standards bodies and alliances: *e.g.,*

- Intel recent History…
  - NIST Cyberphysical Systems Initiative - Data Interoperability WG
  - IETF/IAB Workshop on Semantic Interoperability
  - NSF-Intel ICN-WEN program

(Information Centric Networking in the Wireless Edge Network)

Smart Object Issues

- Frameworks:
  - Standards: So many to choose from!
  - Ontologies: Even more to choose from!
  - Interoperability: What form of interoperability (syntactic, semantics, object, etc.)?
  - How to develop distributed IoT services using metadata?
- Discoverability at scale
- Naming, Lineage and Access
- Semantic Interoperability – does setting a light bulb to "on" give you usable light?
  - Maybe not if lumens output is set really low
  - Maybe if light bulb only has two output levels – off or some set amount of lumens
- Security



Q. Can you turn on a light bulb?

A. Maybe:

- if you use the right standard and
- if you use the right ontology
- or if you have a bridge to another framework and semantics match
- If you can discover the light bulb
- If you can address the light bulb
- If you have permission

Charter

- Assess the Smart Objects landscape and contribute to a living survey
  - Highlight the most relevant models and frameworks
  - Identify commonalities, taxonomies, gaps
- Capture minimal/optimal requirements for Fog-inspired use cases
  - Object framework (e.g., discoverability, bridging, registries)
  - Fog formation
  - Work orchestration
  - Data economy
- Build tools and demonstrate viability of Smart Objects approach
  - POC(s) implemented (on OpenFog testbed)
  - Open Source

Identify, coordinate with, influence, extend, and drive relevant standards

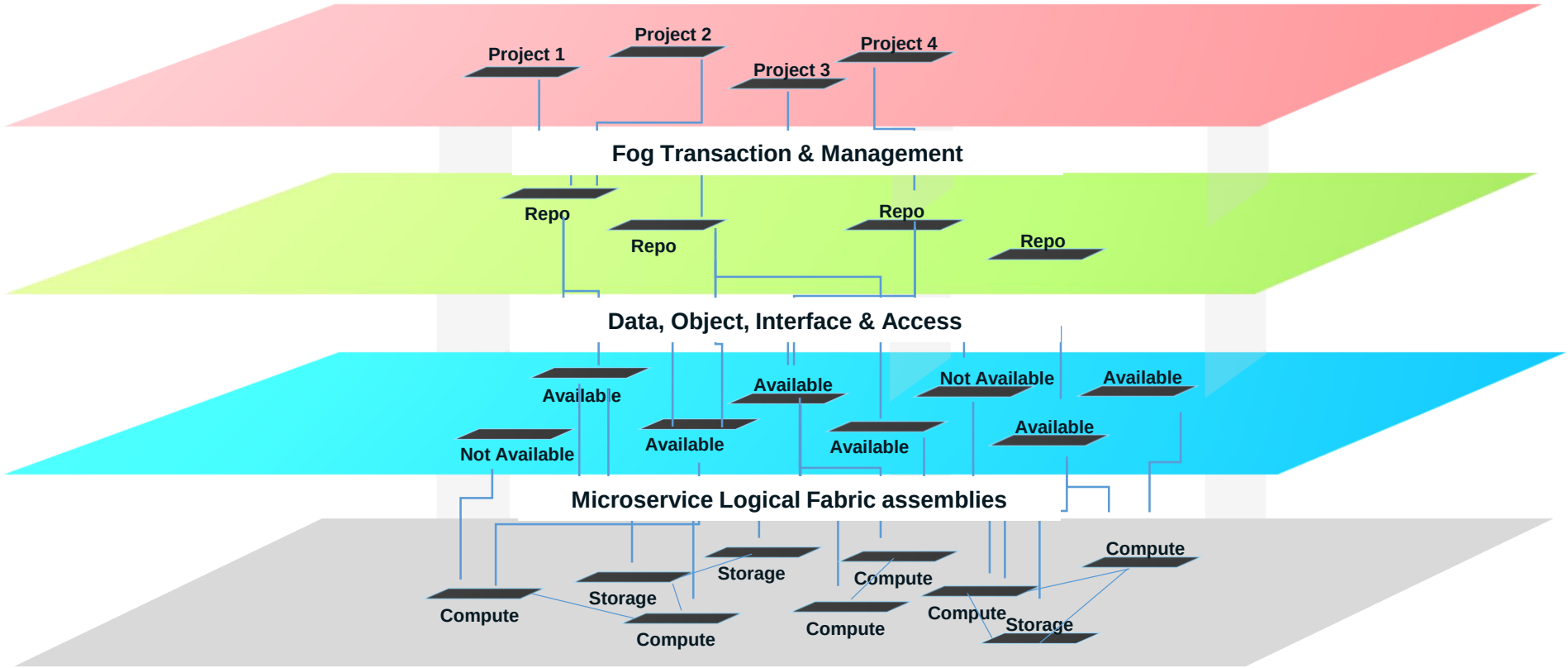
Transaction Management & Orchestration Principles

Katalin KB Walcott – Principal Engineer, Intel IoTG

Intel Fog SW Architecture Technical Lead

katalin.kb.Walcott@intel.com

Logical Transaction Layers – concept



What is a Transaction?

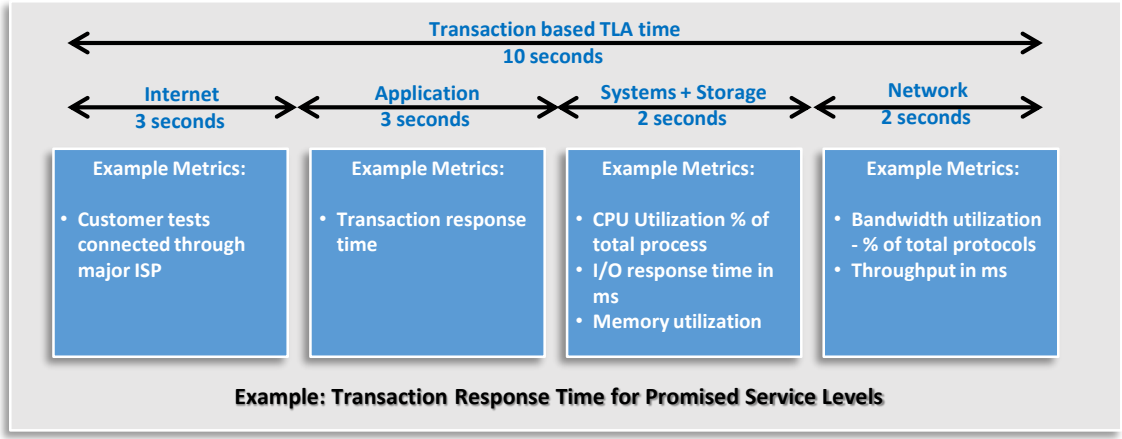
Contract Management of Transaction based Agreements

<Service name> will be available <#%> of time during <hrs> of operation during <hrs> and <days> of the week.

- *Individual service outage in excess of <time period> or <sum> of outages exceeding <time period> will constitute violation*

<#%> of <service name> transactions will exhibit <#seconds> or less response time, defined as the interval from the time the user sends a transaction to the time a visual confirmation of transaction completion is received.

- *Missing the metrics for business transactions measured over any business week will result in a violation.*



Example: Transaction Response Time for Promised Service Levels

Service Elements:

- Include the specifics of services provided:
  - Conditions of service availability
  - Standards such as time windows for each level of service
  - Responsibilities of each party
  - Escalation procedures
  - Cost/service tradeoffs

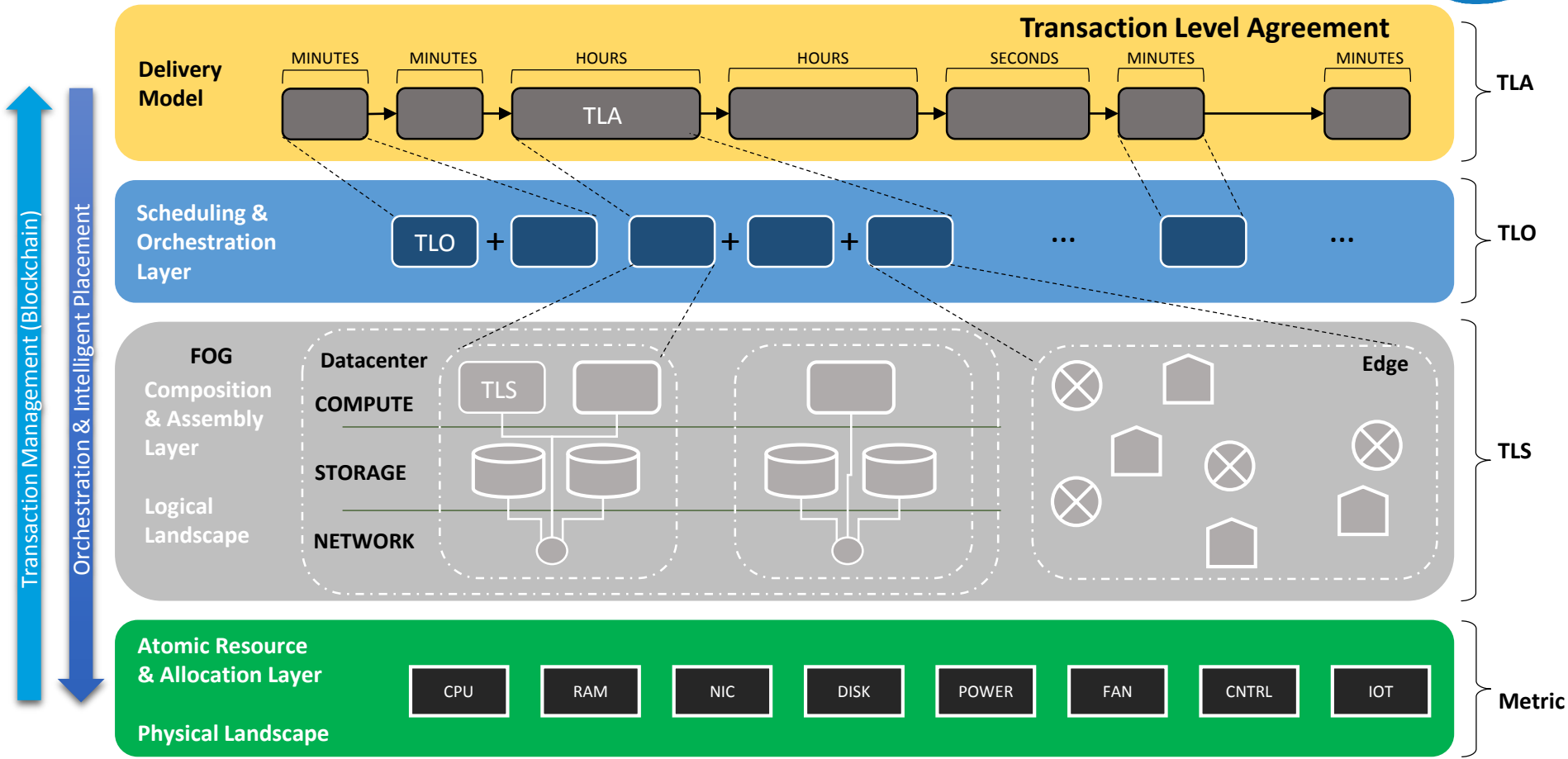
Management Elements:

- Include the definitions of measurements:
  - Methods
  - Standards,
  - Reporting process
  - Content
  - Frequency
  - SLA breaches

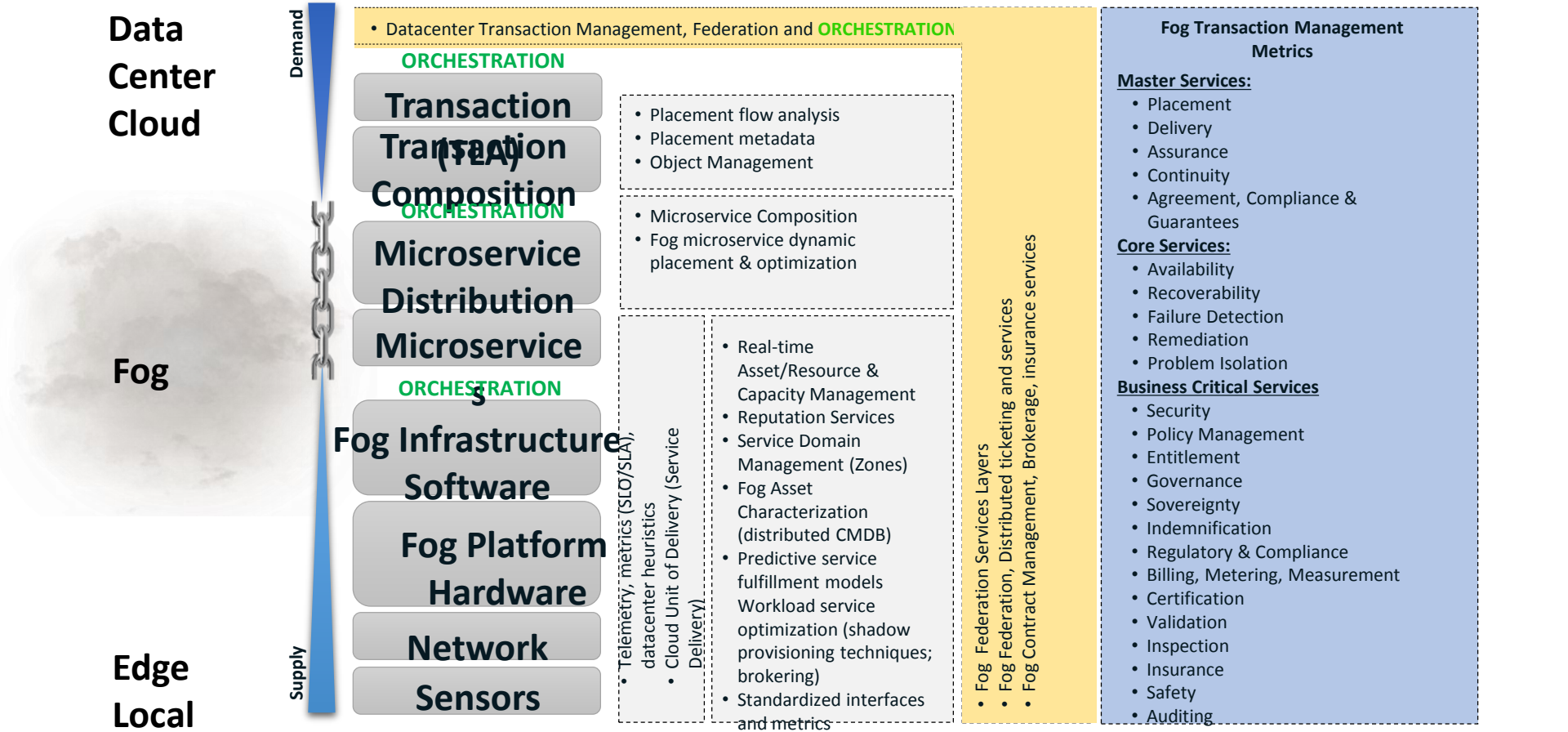
Metrics to Monitor:

- Monitoring schemas may include:
  - Service availability – amount of time the service is available for use
  - Usability – timeliness, transaction completion, latency, refresh rate
  - Delivery - Performance , Availability, Reliability
  - Defect rates – percentages of errors in major deliverable
  - Technical quality – measurement of quality in delivery (time, response rate etc…)
  - Security /Trustworthiness -

Transaction Level Management Elements

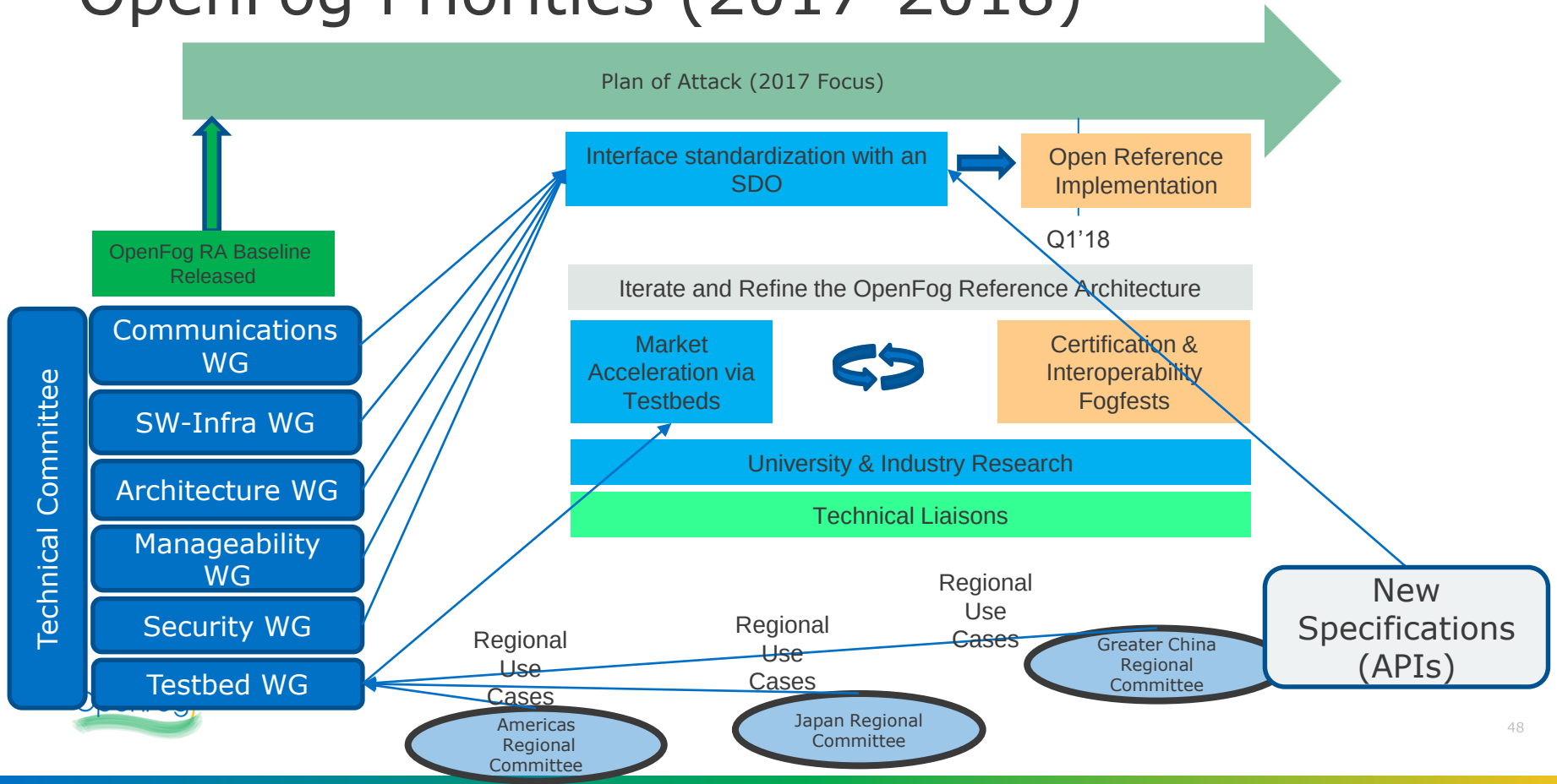


Resource, Data, Object Transaction Management



Moving forward…

OpenFog Priorities (2017-2018)




OpenFog
www.OpenFogConsortium.org