White Paper

OpenFog Architecture Overview

OpenFog Consortium Architecture Working Group
www.OpenFogConsortium.org

February 2016

Executive Summary

The Internet of Things (IoT) is driving a digital transformation in all aspects of our lives and businesses. The growing number of connected devices is creating data at an exponential rate. Current "cloud-only" IoT architectures lead to infrastructure and connectivity limitations and slow adoption and reduce the value that can be realized via this transformational technology. Instead, selectively moving computation, communication, control, and decision making to the network edge where data is being generated is an emerging area of computer science and electrical engineering. This is called fog (or edge) computing.

The OpenFog Architecture is a system-level architecture that extends elements of compute, networking and storage across the cloud through to the edge of the network. This approach is particularly suited to IoT systems and accelerates the decision-making velocity. This architecture serves a specific subset of business problems that can't be successfully implemented using "cloud only" based architectures or relying solely on intelligent edge devices. OpenFog should be thought of as complementary to, and an extension of the traditional cloud based model where implementations of the architecture can reside in multiple layers of a network's topology. The goal of the OpenFog architecture is to facilitate deployments which highlight interoperability, performance, security, scalability, programmability, reliability, availability, serviceability, and agility. Proprietary or single vendor solutions can result in limited supplier diversity, which can have a negative impact on market adoption, system cost, quality and innovation.

The OpenFog Consortium, formed in November 2015, is based on the premise that an open architecture is essential for the success of a ubiquitous fog computing ecosystem for IoT platforms and applications. It is our intent to ensure the OpenFog architecture results in fully interoperable systems, supported by a vibrant supplier ecosystem.

Contents

1 Areas of Opportunity

The Internet of Things (IoT) is driving business transformation by connecting everyday objects and devices together and to cloud-hosted services. Current deployment models emphasize mandatory cloud connectivity, which is not feasible in many real world situations. Moreover, these connected devices are creating data at an exponential rate which will drive performance and network congestion challenges at the edge infrastructure. Current architectural approaches cannot sustain the projected velocity and volume requirements of IoT. To sustain IoT momentum, the OpenFog Consortium is defining a new architecture that can address infrastructure and connectivity challenges by emphasizing information processing closer to where the data is being produced or used. This approach is called fog computing.

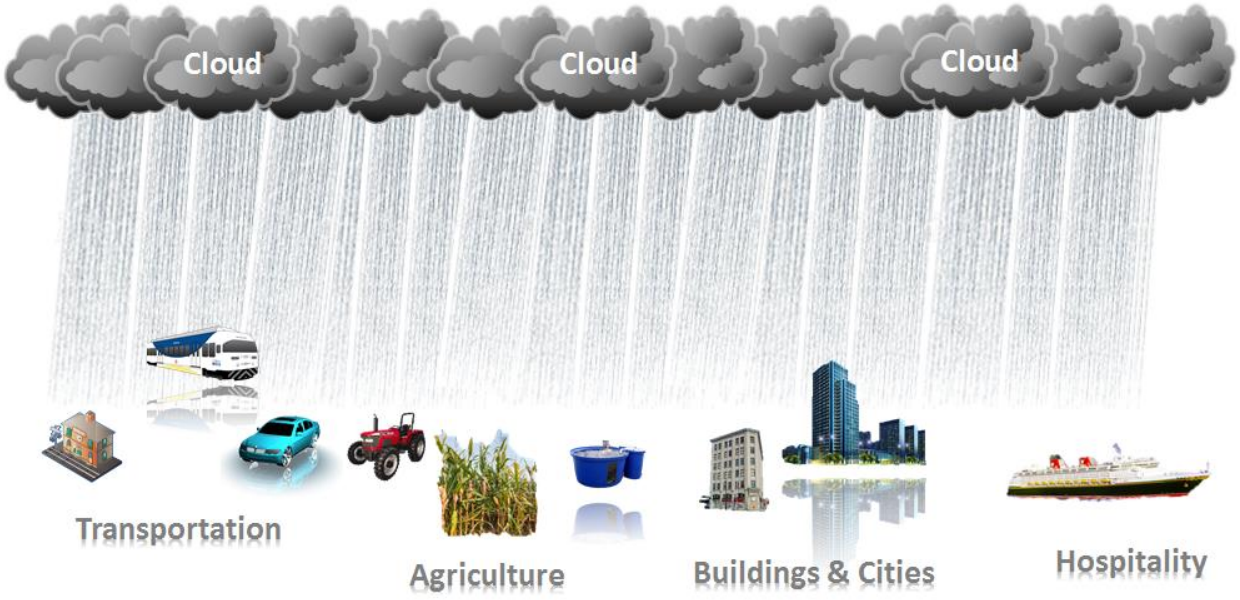

Figure 1 Cloud computing unfettered

The OpenFog architecture represents a shift from traditional closed systems and a reliance on cloud focused models, to a new computational model that moves computation near the edge, and potentially right up to the IoT sensors and actuators of the network based on workload requirements and device capability. Called fog nodes, these are not completely fixed to the edge, but should be seen as fluid system of connectivity. In that context, we believe that OpenFog architecture is complementary to, and an extension of, the traditional cloud based model as implementations can reside in multiple layers of a network's topology which may include a backend cloud.

1.1 The Roles of Edge and Cloud in the OpenFog Architecture

IoT systems are deployed to address key customer concerns and associated use cases and applications. To this end, these systems employ computational intelligence in order to enable a cyber-physical process (CPP) to reach its optimal state by managing the processes through closed-loop systems. A CPP can be characterized by three sets of parameters: parameters that define the desired state, parameters that are observed and parameters that can influence the process state. The computational intelligence can be enabled by a continuum of OpenFog deployments and backend cloud resources which depend on the domain specific scenario being realized.

As an example in IoT, there are at least three broad categories of computational layers: regulatory control, supervisory control and decision support. Conceptually, regulatory control ensures that the process stays close to the desired state. Supervisory control will ensure that the desired state is optimized based on the learnings from the current and past states. Decision support operates on the data accumulated from all the installations and generates insights that can be fed back to the lower level control layers and also into enterprise resource planning (ERP) systems for strategic decision making. Both regulatory and supervisory controls have relatively smaller scopes, usually a single installation. In contrast, decision support operates at the distributed enterprise scale. Depending on the operational systemic qualities, the computational intelligence can span OpenFog and the cloud seamlessly. The decision of computation and its associated location depends on the tolerable latency between a CPP event and actuation.

1.2 OpenFog and other Consortia

The OpenFog Consortium invites open participation from across industry, academia and non-profit organizations which have an interest in the emerging IoT landscape. The OpenFog Consortium intends to harmonize with other groups including, but not limited to, the Industrial Internet Consortium (IIC), ETSI-MEC (Mobile Edge Computing), Open Connectivity Foundation (OCF) and the OpenNFV.

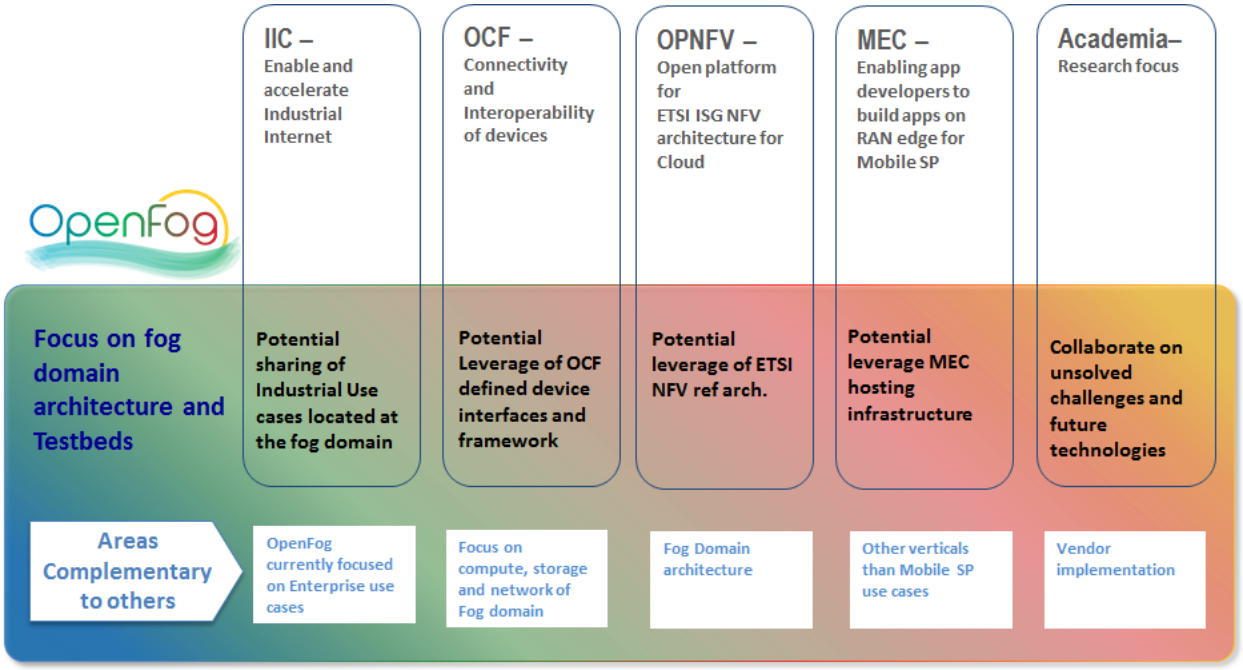

Figure 2 OpenFog and other Consortia

1.2.1 Applications of OpenFog

OpenFog deployments are logically hierarchical in nature from the information processing viewpoint. The hierarchy starts with operational support and ends with decision support processing. An OpenFog architecture is applicable across many different vertical markets including transportation, agriculture, smart-cities, smart–buildings, hospitality, etc. and provides business value for IoT applications that require low latency, are network-constrained, et al. For a brief description of how this architecture could be applied to various vertical markets please visit the appendix. Before going into too much depth, we believe it's important to describe the pillars and key tenets of OpenFog.

1.3 Pillars of OpenFog Architecture

At its core, the OpenFog architecture uses a multitude of computational clients or edge devices. This may operate in concert with associated cloud services to carry out storage, compute, networked communication and associated management tasks optimized based on workload requirements. To highlight the contrast between the OpenFog architecture and traditional cloud architectures, the following properties stand out. Specifically, the OpenFog architecture should:

- Include lower latency storage at or near the end-user and business deployment.
- Perform the required computation near the end-user and data to avoid latency, network and other migration costs (including bandwidth).
- Use low latency communication at or near the end-user rather than requiring all communications to be routed and synchronized through the backbone network.
- Implement elements of management, including network measurement, control and configuration, at or near the endpoint rather than being controlled primarily by gateways such as those in the LTE Core.
- Allow telemetry and locally computed analytics results to be copied to the backend cloud in a secured manner for further analytics and orchestration.

An OpenFog Fabric is made up of nodes or layers that may be distributed, centralized or a combination thereof. It may rely and be implemented on dedicated hardware, software, or both. The common denominator is that this fabric distributes the resources and services of computation, communication, control, and storage across available devices, systems, and clouds to achieve the desired function while meeting all application requirements.

Choosing between a cloud and OpenFog is not a binary decision. They form a mutually beneficial, inter-dependent continuum. In the continuum, the definition of what is cloud and what is endpoint is relative. These devices are interdependent and mutually beneficial: certain functions are naturally more advantageous to carry out in fog while others are better suited to cloud. Traditional backend cloud will continue to remain an important part of computing systems as OpenFog computing emerges. In many of these systems the fog and cloud will both be implemented. The segmentation of what tasks go to fog and what goes to the backend cloud are application specific, and could change dynamically based upon the instantaneous state of the network, in areas like processor loads, link bandwidths, storage capacities, fault events, security threats, etc.

The OpenFog architecture will define fog-cloud and fog-fog interfaces. OpenFog architectures offer several unique advantages, which we term CEAL: (1) Cognition: awareness of client-centric objectives to enact autonomy, (2) Efficiency: dynamic pooling of local unused resources from participating end-user devices, (3) Agility: rapid innovation and affordable scaling under a common infrastructure; and (4) Latency: real-time processing and cyber-physical system control.

Platform as a service (PaaS) is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage web

applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application. OpenFog architecture intends to define the required infrastructure to enable building Fog as a Service (FaaS) to address certain classes of business challenges. The infrastructure and architecture building blocks below show how FaaS may be enabled and will be expanded upon in the reference architecture.

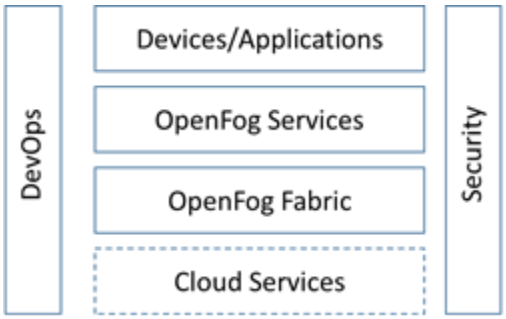

Figure 3 OpenFog Infrastructure View

OpenFog Fabric is composed of building blocks which allow the construction of a homogenous computational infrastructure on which useful services can be delivered to the surrounding ecosystem (e.g. devices, protocol gateways and other fog nodes). The homogenous infrastructure is generally built upon heterogeneous hardware and platforms supplied by multiple vendors.

OpenFog Services are built upon the OpenFog fabric infrastructure. These services may include network acceleration, NFV, SDN, content delivery, device management, device topology, complex event processing, video encoding, field gateway, protocol bridging, traffic offloading, crypto, compression, analytics platform, analytics algorithms/libraries etc. This is an example of a micro-service architecture.

Devices/Applications are edge sensors, actuators, and applications running standalone, within a fog deployment, or spanning fog deployments. This is addressed by the OpenFog service layer.

Cloud Services may take advantage of the cloud for computational work that needs to operate on a larger data scope or pre-processed edge data to establish policies. These should be leveraged in ways that don't impede operational autonomy.

Security is fundamental to OpenFog deployments. Discrete units of functionality within each architecture layer are wrapped with discretionary access control mechanisms so that the OpenFog deployment and the

surrounding ecosystem operate in a safe and secure environment. The OpenFog architecture will ensure all the data transfers between the participating endpoints are secured through the state of the art information security practices.

DevOps are driven by automation enabled by operationally efficient set of standard DevOps processes and frameworks. The DevOps in OpenFog drives the agility of software upgrades and patching through controlled continuous integration processes.

Common themes appear in OpenFog deployments which we represent as pillars of our architecture. Building upon each of these pillars is key to a successful OpenFog implementation. The following sections describe each pillar of the architecture and why we believe it's of critical importance to OpenFog.

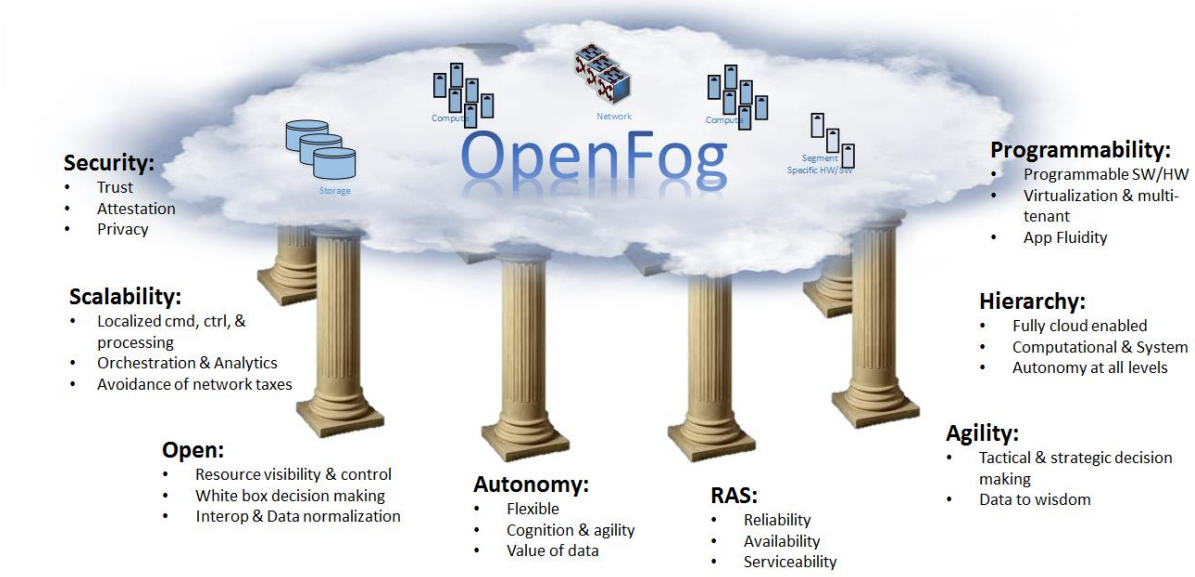

Figure 4 Pillars of OpenFog

1.4 Security

OpenFog deployments can be instantiated on local hardware, migrate across networks, be composed of pure software, or be multi-tenant in nature. As a result, taking an infrastructure viewpoint, fog nodes and fog layers can be seen in some deployments as Fog as a Service (FaaS). With FaaS, the location of a layer and node deployment doesn't always fit within the confines of a single data center, but that doesn't remove the requirements of security or safety. In these scenarios cloud-driven security or proprietary closed security measures aren't always sufficient to protect assets. From this

infrastructure viewpoint both consumer and providers of fog services have associated risks to their assets due to distributed data storage and network topologies.

The Security Pillar starts with a clear definition of base building blocks, or "things." These things must employ a hardware-based immutable root of trust. The root of trust must then be attestable by software agents running within and throughout the infrastructure. Because of the proximity to end users and locality on the edge, nodes in fog networks can often act as the first node of access control and encryption, provide contextual integrity and isolation, and enable the control of aggregating privacy-sensitive data before it leaves the edge. As more complex topologies are created, the attestation continues as a chain of trust throughout the fog node, to other fog nodes and to the cloud for continued security assurance. Since fog nodes may also be dynamically instantiated or torn down, hardware and software resources must be attestable. Components that aren't required or aren't attestable shouldn't be allowed to participate in the fog node or be deemed to have fully trustworthy data.

Security implementations have many different descriptions and attributes such as privacy, anonymity, integrity, trust, attestation, hardware root of trust (HW RoT), verification and measurement. These are key attributes for OpenFog Architecture. Achieving the foundational elements for security requires an approach to discover, attest, and verify all smart and connected "things" before trust can be established. Security runs throughout the OpenFog Architecture and protects assets in infrastructure through data. The privacy aspects of security are also a key concern of OpenFog architectures, as much of the data they process could be private. Security is fundamentally visible and structural throughout all of the verticals targeted by the OpenFog architecture.

1.5 Scalability

The Scalability Pillar is critical to address the dynamic technical and business needs that drive customers to fog deployments. Because of the great variability in the potential use cases of fog, the reference architecture must enable scale to be usable in modest sized deployments, and then seamlessly grow and scale to accommodate the largest, most critical fog networks. This scalability is essential for OpenFog implementations to adapt with the business needs as it relates to system cost and performance. Each OpenFog node is a scale-unit of deployment that can run on its own or as a part of the hierarchical fog fabric. The fabric can be scaled up or down in a demand-driven elastic environment. Storage, networks and analytics services should be able to scale with the fog infrastructure. The scalability which is present

throughout the OpenFog architecture enables fog nodes to provide basic support to address the business requirements and enable a pay-as-you-grow model for the FaaS.

Scalability to address business needs may involve several dimensions in fog networks.

- **Scalable performance** and performance at scale enables growth of fog instance capabilities in response to critical application performance demands (i.e. low latency between sensor reading and resulting actuator responses).
- **Scalable capacity** allows fog networks to grow as more applications, endpoints, "things," users or objects are added to the network.
- **Scalable reliability** and reliability at scale permits the inclusion of redundant fog capabilities to manage faults or overloads and that a large deployment's integrity and reliability scale. This is also part of the OpenFog RAS (Reliability, Availability, and Serviceability) pillar.
- **Scalable security** is also a property of fog networks. Security is a standalone pillar, but in some instances the performance relative to a business' motivation to adopt OpenFog dictates otherwise, and security needs may evolve over time.
- **Scalability of software** and management infrastructures are also vital to OpenFog.

1.6 Open

Openness is essential for the success of a ubiquitous fog computing ecosystem for IoT platforms and applications. Proprietary or single vendor solutions can result in limited supplier diversity, which can have a negative impact on system cost, quality and innovation. The previously-described security pillar shares a common theme and requirements in openness characteristics.

- **Composability** provides a basis for portability and fluidity of apps and services at instantiation. Additional emphasis of composability is visible in the programmability pillar.
- **Interoperability** leads to secure discovery of compute, network, and storage and enables fluidity and portability during execution.

- **Open communication** on a network enables features like pooling of resources near edge network to collect the idle processing power, storage capacity, sensing ability and wireless connectivity within the network and maximize the delivery to the business mission.

- **Location transparency** of instance to ensure nodes can exist anywhere in the hierarchy.

Openness as a foundational principle enables OpenFog nodes to exist anywhere in a network and span networks. This openness enables pooling by discovery such that new software-defined OpenFog nodes can be dynamically created to solve a business mission. The "open" in OpenFog is a pillar to ensure the OpenFog architecture results in fully interoperable systems, supported by a vibrant supplier ecosystem.

1.7 Autonomy

Operational autonomy enables fog deployments to deliver the designed functionality in the face of the external service failures and should be supported throughout the hierarchy. Autonomy at the network edge means intelligence derived by the local devices, and "peer" data can be used to efficiently fulfill the business' mission. Decision making will be made at all levels of a deployment's hierarchy including near the device or higher order layers, but it's no longer required that centralized decision-making occurs only in the cloud. OpenFog supports autonomy for a wide range of functions and by its very nature does not rely upon centralized entity for operation (e.g. backend cloud). Some of the typical areas include:

- **Autonomy of discovery** to enable resource discovery and registration.
- **Autonomy of orchestration and management** automates the process of bringing services online, managing it through the operational lifecycle.
- **Autonomy of security,** one of the most critical considerations for OpenFog. Depicted in the security pillar, OpenFog supports autonomous security functions like AAA (authentication, authorization, and accounting), InfoSec, etc. It enables devices and services to come online, authenticate themselves against security services, and perform their functions to complete the business mission.
- **Autonomy of operation** for localized decision making to keep an IoT system running and fulfilling dynamic business missions.

With OpenFog deployments, DIKW (See glossary) enables localized analytics to drive actions and autonomous decision making nearest the edge.

1.8 Programmability

The Programmability Pillar enables highly adaptive deployments, wherein re-tasking of a fog node or layer (fog cluster), for accommodating operational dynamics, can be completely automated. The re-tasking can be done with the help of the fog cluster's inherent programmability interfaces or with those of higher order fog clusters via intra and inter-fog node communications. The OpenFog Reference Architecture accommodates diverse deployment scenarios through prescriptive standards, technologies, APIs, frameworks and runtime containers so that a domain-specific solution is composed from components suggested in the reference architecture.

Programmability of an OpenFog node includes the following benefits:

- **Adaptive infrastructure** for diverse IoT deployment scenarios and support changing business needs.
- **Resource efficient deployments** to maximize the resources through containerizing the deployments.
- **Multi-tenancy** to accommodate multiple tenants in a logically isolated runtime environment.
- **Economical operations** that result from a high density and adaptive infrastructure.
- **Enhanced Security** to apply patches and react to the evolving threats.

Through these key systemic characteristics, the OpenFog reference architecture will enable a higher degree of programmable automation and scalability required for successful OpenFog deployments.

1.9 RAS (Reliability, Availability, and Serviceability)

RAS is resident throughout successful system architectures and, as such, takes on great importance in the OpenFog Architecture. Hardware, software, and network hierarchy are the three main areas of system RAS.

A reliable deployment will continue deliver designed functionality under normal as well as adverse operating conditions. OpenFog reliability includes but is not limited to the following properties:

- Predicated to the health of the underlying OpenFog platform hardware, software and associated fog network which is usually measured by "uptime."

- Safeguarding the availability of data and compute on edge gateways using enhanced hardware, software and network designs to improve performance and support experiences of OpenFog deployments.
- Autonomous predictive and adaptive self-managing capabilities when required by the health of the system to initiate self-healing routines for hardware and software.

Hardware, software and networking reliability form the basis for availability and serviceability.

Availability enables continuous management and orchestration to ensure the business mission is being fulfilled. The Availability aspects of the RAS pillar is described but not limited by the following key properties:

- Secure access at all levels of a fog hierarchy for orchestration, manageability and control which includes the ability for upgradeability, diagnostics and secure firmware modification.
- Availability also infers that redundant or duplicate devices, services (peer-to-peer) and data storage appear in the end-to-end IoT platform.
- Ability to control all aspects of the underlying hardware on which the OpenFog system is comprised which includes mesh access capabilities of end point sensor/peering, remote boot capabilities of the platform from BIOS to Operating System instance in the hierarchy.

Servicing a fog deployment to ensure correct operation is key for any successful deployment Serviceability of the RAS pillar is described but not limited by the following properties:

- Highly automated installation, upgrade and repair is essential to the ability to efficiently deploy fog at scale
- Serviceability of the system means that as the underlying hardware or software require support. The hardware or software can either autonomously heal or be serviced by the various manufacturers.
- Serviceability of the OpenFog RAS Pillar also implies an ease of use to accommodate maintenance of the OpenFog system deployments.

RAS is especially important for various OpenFog deployments in harsh environmental conditions where we expect this architecture to be deployed. This is why it’s an important pillar of the OpenFog Architecture and why aspects from RAS can be found throughout associated OpenFog implementations.

1.10 Agility

Agility as a key pillar that enables quick and astute business operational decisions for an OpenFog System. The predicted scale of the data generated by IoT means that it is highly unlikely that humans alone will be able to comprehend the data, derive knowledge and make wise decisions about how to best leverage their IoT assets for the benefit of their businesses. In the OpenFog architecture the agility pillar is about making sure that the valuable data generated in the IoT can be rapidly transformed into actionable insights that drive rapid decisions and further levels of automation to support business interest.

Data is key to most information systems and OpenFog architectures are no different. Data generation by sensors and systems in an OpenFog deployment are turbulent, bursty, and are often created in huge volumes. Most importantly, data may not have context. Context is the basis on which operational decisions will be made in the IoT and context is created only when the data is collated, aggregated and analyzed. The analysis of data can of course be done at the cloud layer of the network hierarchy, but this subjects the data to increasing levels of latency, delay and unreliably introduced by multiple layers of delivery networks. The ideal approach is to make all operational decisions as soon as data can be turned into a meaningful context. Contextual understanding of data enables systems to make faster, better decisions.

The OpenFog architecture enables the creation of context from data where both tactical and strategic decisions can be made quickly to maximize operational performance of the system(s). Tactical and quick responding decisions should be made as close to the edge as possible. More strategic, system-wide decisions and policy management are made further up the layers in the fog hierarchy. This avoids network dependencies as described in other OpenFog pillars.

Businesses which construct systems that transform their data into a meaningful context on which to base their operational decisions. With OpenFog, they'll experience new levels of agility. This agility is achieved because IoT system developers, when using the OpenFog Architecture, may create systems where they're free to optimize the placement of their applications decision making components with respect to the data.

1.11 Hierarchy

OpenFog computing resources can be seen as a logical hierarchy based on the functional requirements of an end-to-end IoT system. Depending on the scale and the nature of the domain problem being solved, the hierarchy may constitute a network of smart and connected partitioned systems arranged in physical or logical layers, or it may collapse into a single physical system based on the size and scale of the domain problem (Scalability pillar). Using building automation as an example, a company that manages a single office complex may have the entire fog deployment located locally, while a large commercial property management company may have distributed fog deployments at local or regional levels that feed information to centralized parent systems and services. Each operational fog node is autonomous (Autonomy pillar) to ensure uninterrupted operations of the facility it manages.

The majority of the real world systems are expected to have a mix of fog and cloud, while a minority of the systems may be at either fog or cloud exclusively. Cloud computing is designed to provide on-demand scalability and agility and access to shared resources. The cloud provides Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) sets of capabilities for organizations that require elastic scale, security, compliance and improved economics. Fog computing is designed to provide the ability to analyze data near the edge for improved efficiency (where delays are critical or there is limited bandwidth), or to operate while disconnected from a larger network (autonomy). Fog computing enables different fog instances to communicate with each other, enabling dynamic routing for resiliency and efficiency.

2 Summary

OpenFog is an architectural evolution from traditional closed systems and the burgeoning cloud-only models to an approach that emphasizes computation nearest the edge of the network when dictated by business concerns or critical application the functional requirements of the system. This may be enacted in concert with a traditional backend cloud to enable a complete system that provides intelligence for operational as well as strategic decision making. The OpenFog Consortium was founded on the premise based on open architectures and standards that are essential for the success of a ubiquitous fog computing ecosystem. Proprietary or single vendor solutions can result in limited supplier diversity, which can have a negative impact on system cost, quality, market adoption and innovation. The OpenFog architecture under development will result in fully interoperable systems, supported by a vibrant supplier ecosystem to aid business transformations in the technological revolution.

The OpenFog Consortium is focused on the continued development of the OpenFog Reference Architecture which is supported by the pillars described in this whitepaper. This architecture will be tested through new OpenFog horizontal testbeds which will showcase both the reference architecture in action and how multi-vendor solutions can express the various pillars of OpenFog architecture. The intention is to continue to collaborate with academia and across the industry to speed the transformative business opportunities available with this powerful new computing paradigm called fog computing.

3 Appendix

It is important to describe areas by which this architecture could be applied to various vertical markets for additional business value.

3.1 Transportation

OpenFog is critical in transportation because of three fundamental requirements: low latency, maintaining user privacy, and pooling of resources at different layers. Consider the following example of low latency where: a mesh of fog nodes in an intelligent traffic control system can share the collected traffic information to streamline traffic during peak hours, localize accidents, and re-route traffic away from congested traffic areas. Similarly, the pooling of resources can be extremely lucrative in infotainment systems where fog-based applications on each user's phone and in public transport allow the users to share and stream downloaded content from nearby users without a persistent network connection. Finally, safety systems for automated vehicles, surveillance systems on the roads, and ticketing systems in public transport can collect a lot of information in terms of sensor and video data. These systems ideally should only communicate aggregated data to the cloud to maintain user privacy and conserve user bandwidth smartly. The cloud can extract useful business insights such as where to plan the best routes in longer time scales, but is unlikely to provide the latency guarantees in short time scale. The analytics are distributed across edge and cloud to enable real-time decision making at the edge, and policy control and data insights driven from the cloud.

3.2 Agriculture

Agricultural concerns for OpenFog include but are not limited to meat & dairy production, aquatics, hydroponics, vegetables, rice, corn, BIO crops (including algae), etc. In many geographies, agriculture is optimized and returns are maximized by large corporate farms. These farms are already going through a technology revolution to ensure they have the right crop, apply the correct herbicides and pesticides, and maximize usage of water etc. in efforts to maximize profits and yield. Additionally, smaller farms (<2acre) will play an ever increasing role in our food supply as our global population grows. These smaller farms also have an equal need to maximize the effective use of their resources.

Common themes exist across this segment, which include a lack of reliable or cost effective connections to cloud, complexity of knowing real time effectiveness of herbicide and pesticide usage, animal health, environmental factors including but not limited to water and soil, etc. An even larger concern to this segment is that smaller farmers do not have a dedicated IT staff so even if we connect the farmer to cloud infrastructure it is not clear how they could capitalize on that investment versus pooling resources as they naturally do today.

That said, there is still a great opportunity for localized computational resources to make a positive difference for agriculture.

3.3 Smart Cities

Affecting how people interact and operate within the infrastructure of a city, things, etc. is a natural application of OpenFog architecture. The OpenFog architecture can assist in the efficiency of basic city operations especially for concerns around latency, connectivity, privacy, security, etc. This in turn, enables efficient delivery of even more civic services within existing budgetary constraints. A major issue in establishing smart cities is availability of ubiquitous broadband bandwidth and connectivity. While most modern cities have one of more cellular networks providing adequate coverage, these networks often have capacity and peek bandwidth limits that just meet the needs of their existing subscribers. This leaves little bandwidth for the advanced municipal services envisioned in a smart city or real-time surveillance. OpenFog deployments provide an opportunity to address this concern.

Smart city challenges also include safety and security, critical performance and advanced analytics. Municipal networks may carry sensitive traffic and data (i.e. police dispatches), and operate life-critical systems (e.g. smart transportation collision avoidance applications, first responder communications, etc.), and therefore must be both secure and reliable. Advanced analytics of video monitoring is also key for cities to ensure crime is addressed quickly and effectively. Performing the operations of a smart city in a localized center does not lend itself to successful deployment. Hence an OpenFog architecture provides smart cities with the best opportunity for successfully addressing its needs. Security, data encryption and distributed analytics will have a key role in the intelligent fog infrastructure for Smart Cities.

3.3.1 Buildings

Automation in building management is a classic case that demonstrates the need for edge intelligence and localized processing. A commercial building may contain many thousands of sensors to measure various building operating parameters including temperature, humidity, occupancy, door open/close, keycard readers, parking space occupancy, security, elevators and air quality. These sensors emit telemetry at various intervals that is captured by the on-premise infrastructure and saved in a local storage. Variable Frequency Drives and other controller driven actuators will adjust the building conditions that are deemed to be optimal. As telemetry from sensors comes in, the time sensitive computations to decide if the intake fan to HVAC need to run slower, turn off lights when a room is not occupied, trigger the fire alarm upon sensing fire in the building, turn on fire suppression systems in response to a fire event, or darkening the window shades upon sensing UV radiation in the sunlight need to be done by the infrastructure running in close proximity. The OpenFog deployment model will allow autonomous local operations for control function while a centralized infrastructure allows for the creation of control rooms from which multiple building can be monitored and provide exercised supervisory control. Additionally, long term history of building operational telemetry and control actions can be uploaded to the cloud for answering large scale analytical questions on electricity, water and gas consumption, operational efficiencies, downtime of equipment, effectiveness of preventive maintenance activities and other operational aspects of buildings. The stored operational history can also be used to train machine learning models, which can be used in establishing policies for optimizing building operations by executing the cloud trained global policies in the local fog infrastructure.

For more information, please visit www.OpenFogConsortium.org.

4 Glossary

Term	Definition	Source
Access Control	Means to ensure that access to assets is authorized and restricted based on business and security requirements. *Note:* Access control requires both authentication and authorization.	ISO/IEC 27000:2014
Actuators	"An actuator is a mechanical device for moving or controlling a mechanism or system. It takes energy, usually transported by air, electric current, or liquid, and converts that into some kind of motion."	[Sclater2007]
Address	An address is used for locating and accessing – "talking to" – a Device, a Resource, or a Service. In some cases, the ID and the Address can be the same, but conceptually they are different.	IOT-A
Analytics	Synthesis of knowledge from information.	NIST Interagency Publication 8401-1
Application Software	"Software that provides an application service to the user. It is specific to an application in the multimedia and/or hypermedia domain and is composed of programs and data".	[ETSI-ETR173]
Architecture	"The fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution".	[IEEE-1471-2000]
Architecture Description	Work product used to express an architecture.	[ISO/IEC 42010:2011]
Architecture Framework	Conventions, principles and practices for the description of architectures established within a specific domain of	ISO/IEC 42010:2011

	application and/or community of stakeholders	
Architecture Vision	”A high-level, aspirational view of the target architecture.”	[TOGAF9]
Aspiration	“Stakeholder Aspirations are statements that express the expectations and desires of the various stakeholders for the services that the final [system] implementation will provide.”	[E-FRAME]
Authentication	Authentication is the process of verifying a user’s true identity. This may involve the use of one or more means of proof of identification, also known as factors, such as PIN codes and smart cards.	Nexus IoT Glossary
Authorization	Granting of rights, which includes the granting of access based on access rights.	[ISO 7498-2:1989]
Autonomy	The ability of an intelligent system to independently compose and select among different courses of action to accomplish goals based on its knowledge and understanding of the world, itself, and the situation.	IHMC
Availability	Property of being accessible and usable upon demand by an authorized entity.	ISO/IEC 27000:2014
Business Logic	Goal or behavior of a system involving Things serving a particular business purpose. Business Logic can define the behavior of a single Thing, a group of Things, or a complete business process.	IOT-A
Choreography	Type of composition whose elements interact in a non-directed fashion with each autonomy part knowing and following an observable predefined pattern of behavior for the entire (global) composition.	ISO/IEC DIS 18834-1
Collaboration	Type of composition whose elements interact in a non-directed fashion, each according to their own plans and purposes without a predefined pattern of behaviour	ISO/IEC DIS 18834-1

Confidentiality	property that information is not made available or disclosed to unauthorized individuals, entity, or processes	ISO/IEC 27000:2014
Cloud	Or, "The Cloud," is generally used as shorthand for Cloud Computing. The name "Cloud" comes from the fluffy cloud typically used in Visio-style network diagrams to represent a connection to the Internet.	IoT Guide
Cloud Computing	A general term for the delivery of various hosted services over the Internet. The "as-a-Service" moniker is used for cloud services such as Software-as-a-Service, Platform-as-a-Service and Infrastructure-as-a-Service. The back-end for many IoT devices may be delivered via the Cloud.	IoT Guide
Communication Model	The communication model aims at defining the main communication paradigms for connecting elements. This model provides a set of communication rules to build interoperable stacks, together with insights about the main interactions among the elements of the domain model..	IOT-A
Composition	Result of assembling a collection of elements for a particular purpose	ISO/IEC DIS 18834-1
Constrained Network	A constrained network is a network of devices with restricted capabilities regarding storage, computing power, and / or transfer rate.	IOT-A
Controller	Anything that has the capability to affect a Physical Entity, like changing its state or moving it.	IOT-A
Credentials	A credential is a record that contains the authentication information (credentials) required to connect to a resource. Most credentials contain an user name and password.	IOT-A
Cryptography	Discipline that embodies principles, means, and mechanisms for the transformation of data in order to hide its information content, prevent its	ISO/IEC 18014-2:2009

	undetected modification and/or prevent its unauthorized use	
Device	Physical entity embedded inside, or attached to, another physical entity in its vicinity, with capabilities to convey digital information from or to that physical entity	IIC
Device Endpoint	Endpoint that enables access to a device and thus to the related physical entity.	IIC
Digital Entity	Any computational or data element of an IT-based system.	IOT-A
DIKW	**D**ata gathered becomes **I**nformation when stored and retrievable becomes **K**nowledge. Knowledge enables **W**isdom for autonomous IoT.	
Discovery	Discovery is a service to find unknown resources/entities/services based on a rough specification of the desired result. It may be utilized by a human or another service. Credentials for authorization are considered when executing the discovery.	IOT-A
Edge Gateway	Endpoint that provides an entry point into enterprise or service provider core networks	IIC
Element	Unit that is indivisible at a given level of abstraction and has a clearly defined boundary Note: An element can be any type of entity	ISO/IEC DIS 18834-1
Endpoint	one of two components that either implements and exposes an interface to other components or uses the interface of another component.	ISO/IEC 24791-1:2010
Enterprise	Segment of computing mostly focused at traditional IT and Industrial IT.	OpenFog
Edge Computing	Also referred to as Mesh Computing, this concept places applications, data and processing at the logical extremes of a network rather than centralizing them. Placing data and data-intensive applications at the Edge reduces the	IoT Guide

	volume and distance that data must be moved.	
Fog Computing	Fog computing is a system-level horizontal architecture that distributes resources and services of computing, storage, control and networking anywhere along the continuum from Cloud to Things, thereby accelerating the velocity of decision making. Fog-centric architecture serves a specific subset of business problems that cannot be successfully implemented using only traditional cloud based architectures or solely intelligent edge devices.	OpenFog Consortium
Fog Node	The physical and logical network element that implements fog computing services. It is somewhat analogous to a server in cloud computing.	OpenFog Consortium
Gateway	A Gateway is a forwarding element, enabling various local networks to be connected.	IOT-A
Global Storage	Storage that contains global information about many entities of interest. Access to the global storage is available over the internet.	IOT-A
Identity	Properties of an entity that makes it definable and recognizable.	IOT-A
Industry 4.0	Refers to the fourth industrial revolution, following the first (mechanization of production through water and steam power), second (use of electricity for mass production), and third (use of electronics and IT for automation). Experts believe that the fourth revolutionary leap will entail full computerization of traditional industries. A key element of Industry 4.0 is the Smart Factory marked by adaptability, resource efficiency and ergonomics as well as intelligent processes and communication.	Nexus

	Technological basis are cyber-physical systems and the Internet of Things.	
Industrial Internet	An Internet of things, machines, computers and people, enabling intelligent industrial operations using advanced data analytics for transformational business outcomes.	IIC
Information Model	"An information model is a representation of concepts, relationships, constraints, rules, and operations to specify data semantics for a chosen domain of discourse. The advantage of using an information model is that it can provide sharable, stable, and organized structure of information requirements for the domain context. The information model is an abstract representation of entities which can be real objects such as devices in a network or logical such as the entities used in a billing system. Typically, the information model provides formalism to the description of a specific domain without constraining how that description is mapped to an actual implementation. Thus, different mappings can be derived from the same information model. Such mappings are called data models."	[AutoI]
Infrastructure Services	Specific services that are essential for any IoT implementation to work properly. Such services provide support for essential features of the IoT.	IOT-A
Internet	"The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks of local to global scope that are linked by a broad array	[Wikipedia IN]

	of electronic and optical networking technologies. The Internet carries a vast array of information resources and services, most notably the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail. Most traditional communications media, such as telephone and television services, are reshaped or redefined using the technologies of the Internet, giving rise to services such as Voice over Internet Protocol (VoIP) and IPTV. Newspaper publishing has been reshaped into Web sites, blogging, and web feeds. The Internet has enabled or accelerated the creation of new forms of human interactions through instant messaging, Internet forums, and social networking sites. The Internet has no centralized governance in either technological implementation or policies for access and usage; each constituent network sets its own standards. Only the overreaching definitions of the two principal name spaces in the Internet, the Internet-protocol address space and the domain-name system, are directed by a maintainer organization, the Internet Corporation for Assigned Names and Numbers (ICANN). The technical underpinning and standardization of the core protocols (IPv4 and IPv6) is an activity of the Internet Engineering Task Force (IETF), a non-profit organization of loosely affiliated international participants that anyone may associate with by contributing technical expertise.”	
Internet of Things (IoT)	The digital network is soon going to connect physical objects (“things”),	Nexus

	persons, machines, devices and processes. It is expected that 50 Billion devices will be connected to the Internet by 2020. Contrary to the Internet as we know it, where only persons have digital identities, the Internet of Things equips physical objects with digital identities. The objects are embedded with software, electronics and sensors that allow them to communicate with other objects or persons in the digital or physical world. IoT will transform all industries – it is expected that the new connectivity will set off automation in almost all fields of business. Establishing secure infrastructures and trustworthy identities is vital for the successful deployment of this new kind of network.	
Interoperability	The ability to share information and services. The ability of two or more systems or components to exchange and use information. The ability of systems to provide and receive services from other systems and to use the services so interchanged to enable them to operate effectively together.	[TOGAF 9]
IoT Service	Software component enabling interaction with resources through a well-defined interface. Can be orchestrated together with non-IoT services (e.g., enterprise services). Interaction with the service is done via the network.	IOT-A
Local Storage	Special type of resource that contains information about one or only a few entities in the vicinity of a device.	IOT-A
LTE	Long Term Evolution commonly used in 4G.	
Mobile Edge Computing (MEC)	A standard mostly concerned with equipping computational resources at or near base stations in mobile / cellular networks	MEC

Modularity	A property of network elements where individual capabilities can be added or removed without substantial impact of other components.	OpenFog Connsortium
Multi-tenancy	Software Multitenancy refers to a software architecture in which a single instance of a software runs on a server and serves multiple tenants. A tenant is a group of users who share a common access with specific privileges to the software instance. With a multitenant architecture, a software application is designed to provide every tenant a dedicated share of the instance including its data, configuration, user management, tenant individual functionality and non-functional properties.	Wikipedia
Network resource	Resource hosted somewhere in the network, e.g., in the cloud.	IOT-A
On-device Resource	Resource hosted inside a Device and enabling access to the Device and thus to the related Physical Entity.	IOT-A
Orchestration	Type of composition where one particular element is used by the composition to oversee and direct the other elements. *Note:* the element that directs an orchestration is not part of the orchestration.	ISO/IEC DIS 18834-1
Reference Architecture	A reference architecture is an architectural design pattern that indicates how an abstract set of mechanisms and relationships realizes a predetermined set of requirements. It captures the essence of the architecture of a collection of systems. The main purpose of a reference architecture is to provide guidance for the development of architectures. One or more reference architectures may be derived from a common reference model, to address different	IOT-A

	purposes/usages to which the Reference Model may be targeted.	
Reference Model	A reference model is an abstract framework for understanding significant relationships among the entities of some environment. It enables the development of specific reference or concrete architectures using consistent standards or specifications supporting that environment. A reference model consists of a minimal set of unifying concepts, axioms and relationships within a particular problem domain, and is independent of specific standards, technologies, implementations, or other concrete details. A reference model may be used as a basis for education and explaining standards to non-specialists.	[OASIS-RM]
Reliability	Ability of a system or component to perform its required functions under stated conditions for a specified period of time.	ISO/IEC 27040:2015
Resilience	The condition of the system being able to avoid, absorb and/or manage dynamic adversarial conditions while completing assigned mission(s), and to reconstitute operational capabilities after casualties.	IIC
Resource	Computational element that gives access to information about or actuation capabilities on a Physical Entity.	IOT-A
Requirement	A quantitative statement of business need that must be met by a particular architecture or work package.	[TOGAF9]
Scalability	A property of networks where their capabilities can grow or shrink without undue expense of loss of efficiency	OpenFog Consortium
Sensor	A sensor is a special Device that perceives certain characteristics of the	IOT-A

	real world and transfers them into a digital representation.	
Security	The correct term is 'information security' and typically information security comprises three component parts: ▪ Confidentiality. Assurance that information is shared only among authorized persons or organizations. Breaches of confidentiality can occur when data is not handled in a manner appropriate to safeguard the confidentiality of the information concerned. Such disclosure can take place by word of mouth, by printing, copying, e-mailing or creating documents and other data etc.; ▪ Integrity. Assurance that the information is authentic and complete. Ensuring that information can be relied upon to be sufficiently accurate for its purpose. The term 'integrity' is used frequently when considering information security as it represents one of the primary indicators of information security (or lack of it). The integrity of data is not only whether the data is 'correct', but whether it can be trusted and relied upon; ▪ Availability. Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.	[ISO27001]
Service	Services are the mechanism by which needs and capabilities are brought together	[OASIS-RM]
Storage	Special type of Resource that stores information coming from resources and provides information about Entities. They may also include services to	IOT-A

	process the information stored by the resource. As Storages are Resources, they can be deployed either on-device or in the network.	
System	A collection of components organized to accomplish a specific function or set of functions.	[IEEE-1471-2000]
Thing	Generally speaking, any physical object. In the term 'Internet of Things' however, it denotes the same concept as a Physical Entity.	IOT-A
Unconstrained Network	An unconstrained network is a network of devices with no restriction on capabilities such as storage, computing power, and / or transfer rate.	IOT-A
View	The representation of a related set of concerns. A view is what is seen from a viewpoint. An architecture view may be represented by a model to demonstrate to stakeholders their areas of interest in the architecture. A view does not have to be visual or graphical in nature.	[TOGAF 9]
Viewpoint	A definition of the perspective from which a view is taken. It is a specification of the conventions for constructing and using a view (often by means of an appropriate schema or template). A view is what you see; a viewpoint is where you are looking from - the vantage point or perspective that determines what you see.	[TOGAF 9]
Virtual Entity	Computational or data element representing a Physical Entity. Virtual Entities can be either Active or Passive Digital Entities.	IOT-A
Wireless communication technologies	Wireless communication is the transfer of information over a distance without the use of enhanced electrical conductors or "wires". The distances involved may be short (a few meters as in television remote control) or long (thousands or millions of kilometers for radio communications). When the	[Wikipedia WI]

	context is clear, the term is often shortened to "wireless". Wireless communication is generally considered to be a branch of telecommunications.	
Wireline communication technologies	A term associated with a network or terminal that uses metallic wire conductors (and/or optical fibers) for telecommunications.	[setzer-messtechnik2010]
Wireless Sensors and Actuators Network	Wireless sensor and actuator networks (WSANs) are networks of nodes that sense and, potentially, control their environment. They communicate the information through wireless links enabling interaction between people or computers and the surrounding environment.	[OECD2009]

References

[IOT-A] EU IOT-A Terminology.
Online at: http://www.iot-a.eu/public/terminology/copy_of_term

[AIMglobal] Association for Automatic Identification and Mobility.
Online at: http://www.aimglobal.org/

[AutoI] Information Model, Deliverable D3.1, Autonomic Internet (AutoI) Project.
Online at: http://ist-autoi.eu/autoi/d/AutoI_Deliverable_D3.1_-_Information_Model.pdf

[CCSDS 312.0-G-0] Information architecture reference model.
Online at: http://cwe.ccsds.org/sea/docs/SEA-IA/Draft%20Documents/IA%20Reference%20Model/ccsds_rasim_20060308.pdf

[COMPDICT-M2M] Computer Dictionary Definition
Online at: http://www.yourdictionary.com/computer/m2-m

[E-FRAME] E-FRAME project, available.
Online at: http://www.frame-online.net/top-menu/the-architecture-2/faqs/stakeholder-aspiration.html

[EPCglobal] EPC Global glossary (GS1).
Online at:
http://www.epcglobalinc.org/home/GS1_EPCglobal_Glossary_V35_KS_June_09_2009.pdf

[ETSI-ETR173] ETSI Technical report ETR 173, Terminal Equipment (TE); Functional model for multimedia applications.
Online at: http://www.etsi.org/deliver/etsi_etr/100_199/173/01_60/etr_173e01p.pdf

[ETSI TR 102 477] ETSI Corporate telecommunication Networks (CN); Mobility for enterprise communication.
Online at: http://www.etsi.org/deliver/etsi_tr/102400_102499/102477/01.01.01_60/tr_102477v010101p.pdf

[IEEE-1471-2000] IEEE 1471-2000, "IEEE Recommended Practice for Architectural Description of Software-Intensive Systems"

[ITU-IOT] the Internet of Things summary at ITU.
Online at: http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf

[ISO/IEC 2382-1] Information technology -- Vocabulary -- Part 1: Fundamental terms
Online at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=7229

[ISO 27001] ISO 27001: An Introduction To Information, Network and Internet Security

[OGS] Open GeoSpatial portal, the OpenGIS abstract specification Topic 12: the OpenGIS Service architecture.
Online at: http://portal.opengeospatial.org/files/?artifact_id=1221

[OASIS-RM] Reference Model for Service Oriented Architecture 1.0
Online at: http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf

[OECD2009]: "Smart Sensor Networks: Technologies and Applications for Green Growth", December 2009.
Online at: http://www.oecd.org/dataoecd/39/62/44379113.pdf

[Sclater2007] Sclater, N., Mechanisms and Mechanical Devices Sourcebook, 4th Edition (2007), 25, McGraw-Hill

[setzer-messtechnik] setzer-messtechnik glossary, July 2010.
Online at: http://www.setzer-messtechnik.at/grundlagen/rf-glossary.php?lang=en

[TOGAF9] Open Group, TOGAF 9, 2009

[Wikipedia IN] Internet page on Wikipedia, online at: http://en.wikipedia.org/wiki/Internet

[ROZANSKI2005] Software Architecture with Viewpoints and Perspectives.
Online at: http://www.viewpoints-and-perspectives.info/doc/spa191-viewpoints-and-perspectives.pdf

[Wikipedia WI] Wireless page on Wikipedia.
Online at: http://en.wikipedia.org/wiki/Wireless

[IoT Guide] Internet of Things Guide.
Online at: http://internetofthingsguide.com/d/cloud.htm

[Nexsus] Nexus IoT Glossary.
Online at: https://www.nexusgroup.com/en/glossary/?letter=C

[UF IoT] Universal Framework IoT Glossary.
Online at: https://universalframeworks.com/industrial-internet-of-things-i-iot-glossary/

[AutoI] Information Model, Deliverable D3.1, Autonomic Internet (AutoI) Project.
Online at: http://ist-autoi.eu/autoi/d/AutoI_Deliverable_D3.1_-_Information_Model.pdf
[TOGAF9] Open Group, TOGAF 9, 2009