Toward a Converged OpenFog and ETSI MANO Architecture

M. Yannuzzi*, R. Irons-Mclean*, F. van Lingen*, S. Raghav*, A. Somaraju*, C. Byers*, T. Zhang*, A. Jain*,
J. Curado*, D. Carrera†, O. Trullols†, S. Alonso†,
*Cisco Systems
†Barcelona Supercomputing Center (BSC)

***Abstract*—This paper discusses the complementarity of ETSI's NFV MANO and the reference architecture recently published by the OpenFog consortium. Based on this analysis, we propose a converged model, called a Digital IoT Fabric, which brings together the strengths of OpenFog and ETSI MANO architectures, and applies their combined capability to the IoT space. The advantages of the proposed paradigm are outlined through real examples, with special emphasis on showing how a converged architecture can bridge the technological gap between OT and IT.**

***Index Terms*—Fog computing, OpenFog, Cloud, virtualization, IoT, NFV, MANO, 5G, Multi-access Edge Computing (MEC).**

I. Introduction

The OpenFog Consortium (OpenFog) is an industrial and academic alliance [1] that was launched to accelerate the adoption of fog computing, while addressing the main challenges posed by this new paradigm [2]. OpenFog defines fog computing as a "*horizontal, system-level architecture that distributes computing, storage, control and networking functions closer to the users along a cloud-to-thing continuum*". The consortium has recently published the reference architecture of an open fog computing system [3]. This provides a high-level architecture of the fog nodes, their communications and management and will help drive standardization across the various layers and interfaces specified by the consortium. As shown in Fig. 1-(I), the OpenFog architecture specifies the main components for managing nodes in the cloud-to-thing continuum (or fog continuum), covering aspects such as life-cycle management of fog nodes and services at scale, device heterogeneity, orchestration requirements, data flows, security, availability and reliability. All these actions should be automated as much as possible through programmability and policy definitions.

In parallel, the European Telecommunications Standards Institute (ETSI) [4] has standardized the Management and Orchestration (MANO) architecture [5] for Network Functions Virtualization (NFV) [6], which is a cornerstone for deploying and managing services in NFV environments. At present, MANO focuses mainly on the orchestration and management of Virtual Network Functions (VNFs) and associated resources within datacenters and decentralized locations, called NFV Infrastructure Points of Presence (NFVI-PoPs) [7]. While the concept of NFVI-PoPs is gaining momentum thanks to other emerging technologies leveraging the NFV MANO architecture, such as 5G Radio Access Network (RAN) or Multi-access Edge Computing (MEC) [8], the concept of NFVI-PoPs has not yet reached the fog arena. We believe that service providers, system integrators and enterprises embracing NFV will drive the need to have a unified infrastructure and service management framework that can orchestrate the fog computing domain as well [9].

OpenFog addresses the fog continuum, but specifies neither the orchestration and management system, nor how to manage resources located northbound of the fog continuum (i.e., in the backend). ETSI MANO, on the other hand, is typically hosted in the backend, and it is primarily used for orchestrating and managing service chains stitching multiple VNFs across datacenters and NFVI-PoPs. Figure 1-(II) depicts how these two architectures can complement each other. By repurposing the guiding principles from ETSI MANO and extending them to reach fog domain, the new architecture can elastically scale the capacity on-demand and achieve automation of IoT services across tens of millions of fog nodes in support of tens of billions of smart and connected things.

There are a large number of Over-The-Top (OTT) platforms targeting IoT enabling features [10], [11], but no existing solution focuses on extending ETSI MANO to the fog computing domain. Most of these solutions presume availability of reliable networks and cloud back-end systems supplied by a service provider, with little or no consideration for management and orchestration aspects of the infrastructure itself. In this paper, we propose the fusion of ETSI MANO and OpenFog, thereby enabling uniform management across fog, networks and cloud back-end systems. To this end, we propose a converged architecture, called a Digital IoT Fabric, which is compliant with both the OpenFog and ETSI MANO specifications. The term "fabric" alludes to the fact that our architecture can manage fog, network, and backend nodes indistinctly, hence turning the continuum between the backends and the things into a resource fabric (cf. Fig. 1-(III))—this shall be covered in detail in Section II. In other words, our Digital IoT Fabric perceives resources as a unified computing fabric managed as a single entity in a service-centric way.

One of the main advantages of this approach is that IoT services of very different nature can now coexist and be managed in a uniform way. The fundamental requirements of IoT in terms of connectivity, security, applications and data management can be addressed using one single converged architecture disregarding whether the applications exist in the cloud, network or fog nodes. Unlike our previous work [9], [12], in this paper we specifically address the role and fit of the Open-

978-1-5386-3666-4/17/$31.00 ©2017 IEEE

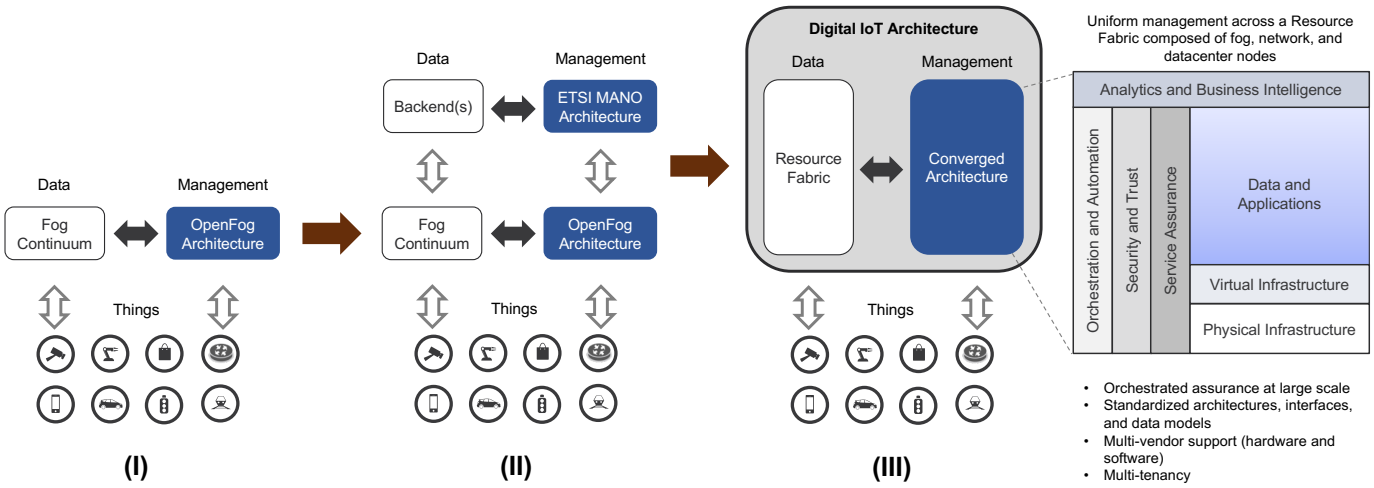

Fig. 1. Natural evolution from the current OpenFog reference architecture (I), toward a converged resource fabric and architecture that merges ETSI MANO and OpenFog capabilities in a seamless way (III).

Fog architecture, as a key enabler to accomplish the expected convergence of IoT, NFV, 5G, and fog.

The rest of the paper is structured as follows. Section II introduces the converged architecture. Section III discusses how this architecture can help bridge the technological gap between OT and IT, and outlines its application in two different scenarios: i) uniform security for industries relying on the Purdue model of control and the ISA/IEC-62443 standards [13]; ii) Smart Cities, highlighting a real deployment in the city of Barcelona, Spain as an example use case for the proposed architecture. Finally, Section IV concludes the paper.

II. A Digital IoT Fabric

The proposed architecture is illustrated in Fig. 2. The left-hand side shows the demarcation between the fog continuum and the datacenters hosting not only the ETSI MANO components but also the Virtual Functions (VFs) and Virtual Infrastructure (VI) for the IoT service backends. In our model, we slice and separate the OpenFog reference architecture [3] into four constituent blocks: 1) the sensors, actuators and control subsystems located southbound of the fog nodes at the very edge of the cloud-to-thing continuum; 2) the core components and layers within any fog node in the cloud-to-thing continuum; 3) a set of cross-cutting capabilities that, as we shall show later in this section, are now extended to manage resources across the entire fabric; and 4) the User Interface (UI) and higher-level management services offered to the different administrators and operators, assuming a multi-tenant environment. Due to space limitations, we cannot comprehensively cover all the elements of the OpenFog and ETSI MANO architectures, so we will focus on how these two can be merged, and examine the touch points enabling their convergence. For an in-depth analysis of the OpenFog and ETSI MANO architectures, the reader is referred to [3] and [5] respectively.

As shown in Fig. 2, we adhere to the Node, System, and Software "Views" as well as the cross-cutting capabilities—denoted as "Perspectives"—as defined by the OpenFog Consortium. These Perspectives enable basic aspects, such as manageability, security, performance and scaling mechanisms, data analysis and control, as well as Business Intelligence (BI) and cross-fog applications. It is worth observing that both NFV and fog-centric services will require such cross-cutting capabilities. Thus, instead of duplicating roles and functionality, in our model these Perspectives amalgamate the capabilities required to handle and scale services across a resource fabric composed of fog, networks and hybrid clouds (i.e., backends that might be hosted combining private and public datacenters).

An adequate combination of Role-Based Access Control (RBAC) and a feature-rich northbound API of the NFV Orchestrator (NFVO) can offer a flexible multi-tenant framework, where a single instance of the Digital IoT Fabric can serve multiple clients, and cover IoT services across different industry verticals and individual services spanning multiple fog nodes and levels of a fog hierarchy. Under this model, the ETSI MANO module can orchestrate and manage instances not only in the backend but also in the fog domain for different clients—these instances are denoted in Fig. 2 as VFs, and VFs*, respectively. Observe that, rather than talking about VNFs, we generalize this concept and instead use the term VFs, since a service chain in IoT will be comprised of virtual functions that will go beyond network-centric functionality [9]. Current ETSI MANO implementations are based on a three-tier model: i) the NFVO; ii) a set of Virtual Network Functions Managers (VNFMs); and iii) a Virtual Infrastructure Manager (VIM). As in the case of the VFs, instead of talking about VNFMs, we use the term Virtual Functions Managers (VFMs). The left-hand side of Fig. 2 shows how ETSI MANO can now instantiate VFs in the virtual infrastructure offered by the backend (VI), as well as in the one offered by fog (VI*). For further details on possible technologies enabling these instantiations from ETSI MANO, the reader is referred to [9], and [12].

The instantiation of VFs* in the fog domain requires interfacing with the OpenFog architecture. These interactions are enabled through the two interfaces shown on the right-hand side of block (2) in Fig. 2 (i.e., between MANO and the OpenFog Node Management layers). OpenFog defines two

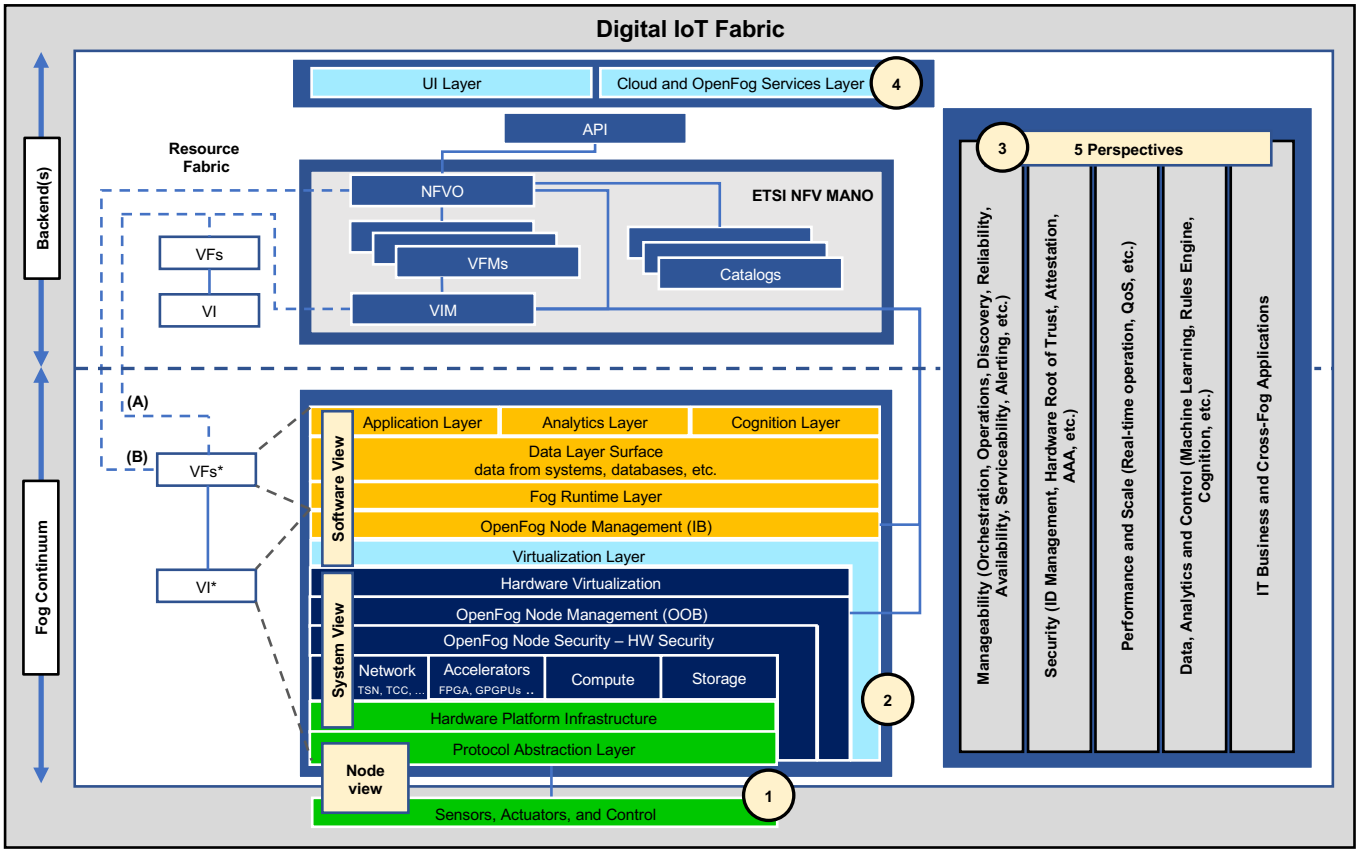

Fig. 2. Digital IoT Fabric: Converged model based on the fusion of the OpenFog and ETSI MANO architectures (the former is split into blocks (1)–(4)).

different OpenFog Node Management layers allowing out-of-band (OOB) management mechanisms and in-band (IB) ones. OOB mechanisms refer to manageability functions that do not run on the host operating system. These generally encompass management mechanisms that can survive all power states, such as the ones defined by the Intelligent Platform Management Interface specification (IPMI) [14]. IB mechanisms refer to manageability functions that are visible to the software and firmware running on a fog node. For instance, the process to spin up a Virtual Machine (VM) or a Linux Container (LXC) in a fog node from the backend requires IB management.

The process for commanding the instantiation of a virtual function, VF*, in the fog virtual infrastructure, VI*, can be accomplished in different ways. Two possible schemes, illustrated as (A) and (B), are shown in Fig. 2. Scheme (A) is based on the traditional NFVO/VFM/VIM combo, which means that the fog node becomes a compute element managed by the VIM. This requires a client that could run as an agent in the fog node. Although there are no technical barriers for implementing scheme (A), commercial support might be an issue in practice, since existing VIMs, such as OpenStack or VMware, might not be willing to extend their support beyond the walls of a datacenter. Scheme (B) offers more flexibility in the fog domain, as the fog node can now be registered and managed directly by the NFVO. In other words, the VFM/VIM functionality can now be distributed, embedded, and autonomously managed by the fog nodes, while still adhering to the ETSI MANO standard. Clearly, this scheme does not require commercial extensions to legacy VIMs.

III. Bridging the Gap between OT and IT

Operational Technology (OT) systems have been traditionally used to monitor events and devices, typically using local non-networked intelligence to control physical elements and processes. OT is often associated with manufacturing and industrial environments and relies both on industry standard protocols as well as proprietary ones, which were developed with strong focus on control and actuation systems. Information Technology (IT), on the other hand, refers to a spectrum of technologies including hardware, software and networked services used to create, process and store digital data. As we shall describe later in Section III-A, the Purdue Model of Control [15] shown in Fig. 3 reflects this distinction, with Levels 4 and 5 related to IT management systems and Levels 0 to 3 related to OT management systems.

Traditionally, IT and OT technologies have co-existed with the application areas distinctly separated and with different management systems and operational methodologies. However, the convergence of OT and IT seems inevitable [10], [11]—although the extent and timing of this convergence is not well understood yet. To deliver transformational operational use cases, such as real time analytics and autonomous decision making for machine health monitoring, a next generation management system will be required, and it will need to cover the full IoT stack (i.e., infrastructure, operating systems, applications, data pipeline, service assurance, security, etc.).

As a result, IT-centric services must be deployed alongside OT services, to generate business value. As such, IT capabilities are becoming operationalized, and pushing the boundaries of traditional architectures, meaning we are now seeing more and more converged standards, such as Open Process Automation [16].

The integration of IT and OT poses complex challenges. From an IT perspective, we can identify two crucial issues:

- IT Security in brownfield scenarios: Many OT systems are already deployed in the field and have little or poor security features that are important for integration into IT systems (e.g. random number generators, ability for secure firmware updates, etc.). Furthermore, security breaches in OT domains can propagate further through the IT domains.
- Protocol Suites: OT systems often grew organically, designed to solve specific industrial use cases. This resulted in the presence of a plethora of protocols and devices in the field, which have never been managed by IT.

The risks of integration from an OT perspective are as follows:

- Safety and physical risk: Industrial operations require a level of reliability in the control and data-delivery planes that traditional IT systems cannot guarantee. This is particularly important in safety applications or when controlling potentially dangerous systems.
- Determinism and low latency: Many industrial automation systems depend on local control loops for monitoring sensors and triggering actuation. Hence, it is crucial to ensure deterministic network latency between the control applications and the sensing and actuation points.
- OT Security: With OT devices gaining network connectivity, the devices are also exposed to security attacks. So systems need to be redesigned taking into consideration the possibility of new security threats from connected networks. The consequences of security breaches in critical OT systems are potentially severe and could even be life threatening.

Clearly, a coordinated mechanism is needed to help resolve these challenges. While the OpenFog architecture can bring IT capabilities to the field (i.e., compute technologies close to the sensors/actuators in an IT-managed way), a converged OpenFog/ETSI MANO architecture can offer automation and uniform life-cycle management of IoT services along a resource fabric spread across the OT and IT domains. Existing ETSI MANO implementations use data modeling languages—predominantly YANG [17]—to model not only domain specific devices/protocols but also services to capture business requirements [5]. This allows the introduction of an "abstraction layer", which implies that the details of the device protocols are not known to the management systems. Therefore, market/vertical specific "function packs" can deploy the full IoT stack for a use case through service automation, at the touch of a button [9], [12]. We contend that, with the penetration of IoT, fog computing along with automated orchestration will play a crucial role in unifying a number of management processes across OT and IT.

We proceed to describe how the Digital IoT Fabric can pave the way for the OT/IT convergence, by analyzing its application in two different areas, industrial security and Smart Cities.

A. Security subject to the Purdue Model in Industry

IEC 62443 [13] is the most widely adopted cyber-security standard for Industrial Control Systems (ICSs). Evolving from the 1990s, where the Purdue Reference Model [15] and ISA 95 [18] established a strong emphasis on security architectures using segmented levels for control system deployments (cf. Fig. 3). This was further developed through ISA99 [19] and IEC 62443, bringing additional risk assessment and business processes focus. The security risk assessment identifies what is defined as critical control, non-critical control, and non-control systems. Each type is treated differently from a security perspective, based on risk.

The majority of security technologies deployed in OT environments are IT-centric, typically enforced as part of IEC 62443-3-3 (system security requirements and security levels). This poses a skillset challenge for OT staff, with IT-centric skills needed to deploy the networking, infrastructure, and compute technologies that OT needs to operate. This poses challenges around who (IT or OT) owns which use cases and services, and where the IT and security skills should reside. With IT services often viewed as being complex by OT teams, automation masks any complexity and minimizes the need for IT knowledge. Ensuring the orchestration system is multi-tenant capable, the operation, visualization, and management of the IT/OT use case can be securely broken out into different services that can be seen by different users. This way, the same service deployment can present different capabilities and views to the IT or OT teams.

The automated IoT platform allows the deployment and enforcement of mixed IT/OT use cases, while enforcing the Purdue Model architecture, and the IEC 62443 foundational security requirements (see Fig. 4). In practice, most use cases deployed in this manner are for monitoring and reporting purposes and not control, however the technology exists to do both. Edge processing and OT use cases can be implemented in a secure and reliable way, accelerating the deployment of business transforming services in fog and industrial IoT environments.

B. Managing IoT services across heterogeneous Fog nodes

This section describes how the Digital IoT Fabric architecture is enabling OT and IT integration in the city of Barcelona.

Fig. 3. Purdue Model of Control Hierarchy.

This initiative started as a co-innovation project with the City Council and other partners, where we demonstrated how various IoT services deployed and operated by different city departments could be uniformly managed throughout the city [9], [12]. In Barcelona, there are more than 3,300 street cabinets. These cabinets form a natural infrastructure for Smart City services offering a single, extensible and distributed platform from edge to cloud. Several OT systems can be connected to (or through) the cabinets across the city, including cameras, lighting elements, multiple controllers, as well as sensors of different nature (e.g., for monitoring noise, the status of the cabinet doors, power, air quality, temperature, etc.).

From an OT standpoint, one of the main challenges in a Smart City is to cope with the deployment and operation of an increasing number of technologies that the different city departments need to install in the field. For instance, the equipment that can be hosted and powered within a cabinet is limited by the size and design on the latter. From an IT standpoint, the main challenges are: a) the risk of "silofication" of data, software and hardware; and b) the complexity and overhead of managing the life-cycle of a large number of services end-to-end across the city.

The role of fog is crucial to address these challenges, as fog nodes placed inside the cabinets can virtualize, aggregate and run multiple applications concurrently and reliably, thereby serving the needs of different city departments (tenants) in a consolidated way. However, fog per se is not sufficient. IT departments in many major cities are realizing that, the way to scale in a cost-effective manner is to bring uniform automation, security, service assurance, data sharing policies and best practices, as common elements serving all city departments. Through a common infrastructure endowed with proper orchestration and RBAC, IT departments can break down the silos and control which OT team has access to what and when [12]. Therefore, a converged architecture, like the one shown in Fig. 2, can not only offer service management capabilities cohesively across fog, network, and backend nodes but also facilitate the desired convergence of OT and IT in cities. Additionally, it allows the data sharing among various smart services using a local fog node to improve the service features such as emergency response time.

As shown in Figure 5 in a Proof-of-Concept (PoC) industrial PCs were deployed as high-end fog nodes inside the street cabinets. Different devices (things) support different interfaces and protocols, which, in the case of Barcelona, were connected

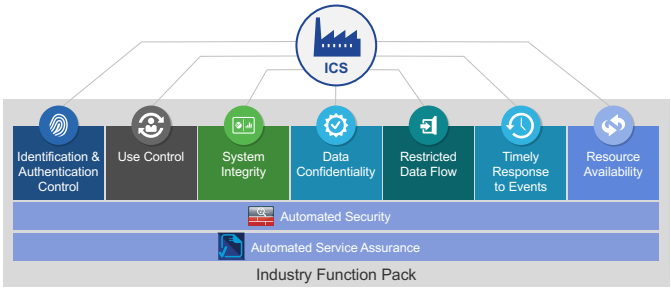

Fig. 4. Automating Security Services.

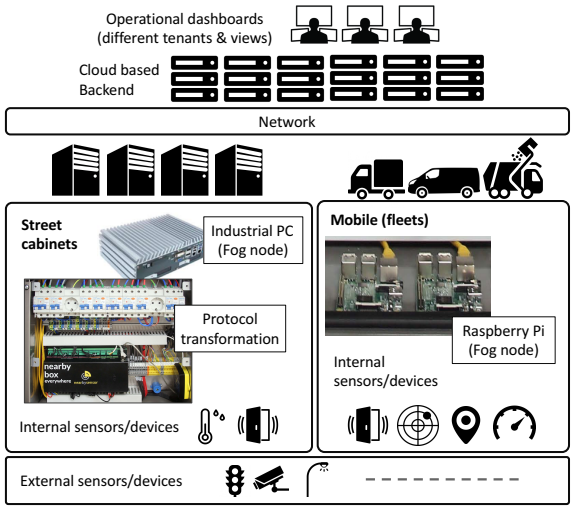

Fig. 5. High-end static fog nodes and low-end mobile fog nodes managed by the Digital IoT Fabric (a single platform to share services and data).

through the NearbySensor box [20] shown at the bottom left of Fig. 5. This box allows to connect different families of wired sensors and controllers to the fog nodes, while normalizing the data to formats that can be shared—based on configured data policies—by different virtualized processes hosted on the fog nodes. For further details on the implemeted PoC, please refer to our previous work [12]

In a separate use case, involving city-owned vehicles, one of the requirements was to also cover use cases in vehicles owned by the city. To this end, we showed the feasibility of using Raspberry Pis [21] as a low-end and highly versatile fog nodes embarked in fleets (cf. the right-hand side of Fig. 5). Observe that, by using converged architecture, we are able to accommodate different classes of fog nodes—whether static or mobile—and integrate them into a single (managed) infrastructure. Essentially, with the architecture depicted in Fig. 2, one can use the YANG standard for modeling both nodes and IoT services, and orchestrate and manage them in an uniform way, irrespective of the node location.

IV. Conclusion

In this paper, we proposed an architecture, called a Digital IoT Fabric, that is compliant with both the OpenFog Consortium reference architecture and ETSI MANO specifications. This novel architecture perceives both cloud and fog fused as a unified computing fabric managed as a single entity in a service-centric way. The architecture allows the automated and homogeneous orchestration of edge, fog, network, cloud nodes, applications running on these nodes, their interfaces and data planes while guaranteeing end-to-end security. We argue that fog computing along with our proposed architecture will be a key to enable the convergence of the IT and OT domains.

Acknowledgments

The authors would like to thank the city of Barcelona, NeabrbySensor, as well as H. Antunes, M. Kranz, R. Zheng, F. Osman, and J. Greengrass.

REFERENCES

[1] "Open Fog Consortium," https://www.openfogconsortium.org/, accessed: 2017-06-15.

[2] F. Bonomi, R. Milito, J. Zhu, and P. Natarajan, "Fog Computing: A Platform for Internet of Things and Analytics," in *Big Data and Internet of Things: A Roadmap for Smart Environments in series Studies in Computational Intelligence*, vol. 546, 2014, pp. 169–186.

[3] "OpenFog Reference Architecture for Fog Computing," https://www.openfogconsortium.org/wp-content/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL.pdf, accessed: 2017-06-19.

[4] "European Telecommunications Standards Institute," http://www.etsi.org/, accessed: 2017-06-15.

[5] "Network Funcitons Virtualisation (NFV), Management and Orchestration," http://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/009/01.01.01_60/gs_NFV-IFA009v010101p.pdf, accessed: 2017-06-15.

[6] "Network Function Virtualisation," http://www.etsi.org/technologies-clusters/technologies/nfv, accessed: 2017-06-15.

[7] "Network Functions Virtualisation (NFV); Use Cases," http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf, accessed: 2017-06-20.

[8] "ETSI Multi-access Edge Computing," http://www.etsi.org/technologies-clusters/technologies/multi-access-edge-computing, accessed: 2017-06-19.

[9] F. van Lingen, M. Yannuzzi, A. Jain, R. Irons-Mclean, O. Lluch, D. Carrera, J. L. Pérez, A. Gutierrez, D. Montero, J. Martí, R. Masó, and J. P. Rodríguez, "The unavoidable convergence of NFV, 5G and Fog: A model-driven approach to bridge Cloud and Edge," in *to appear in IEEE Communications Magazine, special issue on Fog Computing*, vol. 55, no. 8, August 2017.

[10] "Gartner Inc. The Platform Architect's Guide to Designing IoT Solutions," https://www.gartner.com/doc/3153929/platform-architects-guide-designing-iot, accessed: 2017-06-19.

[11] "Gartner Inc. Survey Analysis: 2016 Internet of Things Backbone Survey," https://www.gartner.com/doc/3563218/survey-analysis–internet-things, accessed: 2017-06-19.

[12] M. Yannuzzi, F. van Lingen, A. Jain, O. Lluch, M. Mendoza, D. Carrera, J. L. Pérez, D. Montero, P. Chacín, A. Corsaro, F. Parodi, and A. Olivé, "A New Era for Cities with Fog Computing," in *IEEE Internet Computing Magazine, special issue on Fog Computing*, vol. 21, no. 2, March 2017, pp. 54–67.

[13] "The 62443 Series Overview," http://isa99.isa.org/Public/Information/The-62443-Series-Overview.pdf, accessed: 2017-06-19.

[14] "Intelligent Platform Management Interface Specification v2.0 rev. 1.1, October 2013," https://www.intel.com/content/www/us/en/servers/ipmi/ipmi-second-gen-interface-spec-v2-rev1-1.html, accessed: 2017-06-20.

[15] "Purdue Model of Control, Cisco 2015," http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG/CPwE_chapter2.html, accessed: 2017-06-19.

[16] "Open Process Automation," http://www.opengroup.org/open-process-automation, accessed: 2017-06-19.

[17] "YANG – A Data Modeling Language for the Network Configuration Protocol (NETCONF), RFC 6020, IETF," http://www.rfc-editor.org/rfc/rfc6020.txt, [online; accessed May 10, 2017].

[18] "ISA95, Enterprise-Control System Integration," https://www.isa.org/isa95/, accessed: 2017-06-19.

[19] "ISA99, Industrial Automation and Control Systems Security," https://www.isa.org/isa99/, accessed: 2017-06-19.

[20] "NearBySensor," http://www.nearbysensor.com/, accessed: 2017-06-19.

[21] "RasberryPi," https://www.raspberrypi.org/, accessed: 2017-06-19.