VirtuWind: Virtual and Programmable Industrial Network Prototype Deployed in Operational Wind Park

Toktam Mahmoodi[a], Vivek Kulkarni[b], Wolfgang Kellerer[c], Peter Mangan[d],
Spiros Spirou[e], Ioannis Askoxylakis[f], Xavier Vilajosana[g], Hans Joachim Einsiedler[h], Jürgen Quittek[i]

[a]King's College London, UK, [b]Siemens, Germany, [c]Technical University of Munich, Germany, [d]Intel, Ireland,
[e]Intracom Telecom Greece, [f]FORTH-ICS, Greece, [g]Worldsensing, Spain, [h]Deutsche Telekom AG, Germany, [i]NEC, Germany

***Abstract*— With anticipated exponential growth of connected devices, future industrial networks require an open solutions architecture facilitated by standards and a strong ecosystem. Such solutions should also deal with range of quality of service (QoS) requirements imposed by industrial networks. Preserving strict QoS is particularly challenging when services pass across domains of multiple provides. VirtuWind[1] aims to develop and demonstrate an SDN and NFV ecosystem, based on an open, modular and secure framework to address stringent requirements of the industrial networks. A prototype of the framework for intra-domain and inter-domain scenarios will be showcased in real Wind Parks, as a representative use case of industrial networks. This paper details this vision and explains steps forward.**

***Keywords*—SDN; NFV; industry networks; deterministic networking**

I. INTRODUCTION

In contrast to the traditional network services, industrial applications impose strict Quality of Service (QoS) requirements which imply deterministic forwarding capabilities of the underlying networks. Strict packet latency and jitter bounds, zero packet loss and guaranteed bandwidth are among such requirements. Modern industrial networking technologies exploit closed and (semi-) proprietary protocol stacks and network management systems (NMS). To guarantee stringent industrial-grade QoS requirements, such technologies typically modify and adapt L2 protocols (e.g. Ethernet) by, for instance, exploiting a provider/consumer model for data exchange[2] or master/slave logical architectures with on-the-fly process data insertion into shared frames[3]. However, together with QoS requirements guarantees, they impose limitations on physical and logical network topologies, on service granularity and infrastructure sharing capabilities. Additionally, these approaches limit interoperability between communication equipment of different vendors and their NMS and, consequently, end-to-end service provisioning capabilities.

On the other hand, there is a trend in communication networks in general, to move away from closed, implementation-specific solutions towards more open solutions. Examples of those solutions in today's networks are Software Defined Networking (SDN) and Network Function Virtualization (NFV). SDN aims to increase cross-vendor interoperability and to simplify programmability of services by abstracting the functionality into several planes and specifying open interfaces between them [1]. SDN has also been exploited widely in different domains such as wide area networking and in mobile and wireless networks [2, 3]. At the same time, current SDN deployments exploit traditional QoS models (e.g. DiffServ) which do not ensure the deterministic forwarding required by industrial networks and provide only coarse-grained classes of services. In addition, NFV together with the SDN aim to virtualize network functionalities and networking devices so as to provide programmable connectivity, rapid service provisioning and facilitate service chaining.

Several recent efforts in the research community showed a possibility of service provisioning with bounded packet latency in legacy network architectures under a single control entity [4, 5]. While such approaches may be transferred seamlessly into the SDN architectures [6], the SDN/NFV paradigm brings a potential space for improvements and technological enhancements. The centralized control plane and Virtual Machine (VM) mobility may improve efficiency in network utilization and service availability. Additionally, issues such as control and data plane scalability and availability, efficient service programmability [6] and multi-tenancy [7] are yet to be addressed. To this end, VirtuWind aims to extend existing SDN and NFV architecture enabling industrial-grade QoS capabilities within a single domain as well as across multiple domains by introducing additional controller building blocks, interfaces and protocols. These extensions will then be validated through prototyping and lab testing.

In this paper, we first describe our vision and ambition in deploying a fully re-configurable network in critical infrastructure (Section II). Afterwards, requirements of such networks are elaborated in Section III. Specific challenges in the Wind Park are detailed in Section IV. Section V explains design of an SDN/NFV–based Wind Park network to address existing challenges. Section VI focuses on the technological innovation as well as business and economic impact. Finally, section VII summarizes the paper.

II. VISION AND AMBITION

The wind power industry has been selected as a representative example of industrial networks with strict

[1] VirtuWind: http://www.virtuwind.eu
[2] PROFINET: http://www.profibus.com/technology/profinet/
[3] ETHERCAT: https://www.ethercat.org/default.htm

performance, security, and reliability requirements (Figure 1). As such, the corresponding solutions for VirtuWind will be applicable to other industries such as automotive, smart grid, smart cities and other mission critical applications of the next generation mobile networks, a.k.a. 5G networks, such as the Tactile Internet.

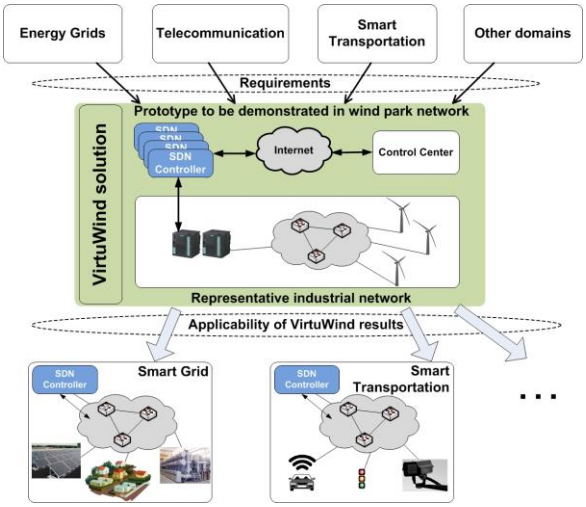

Figure 1: Wind Park network architecture

The Wind Park network is part of a Supervisory Control and Data Acquisition (SCADA) system that regulates power production from each wind turbine and from the entire park. The SCADA system extends beyond the Wind Park with pre-provisioned paths over the Internet to a remote control centre. Moreover, this network interconnects sensors and actuators and a hierarchy of purpose-built controllers and repositories via domain-specific protocols (e.g., IEC 104[4], MODBUS[5]) in a static and secure topology. The challenge is to maintain performance, security, and reliability of the network while making it flexible and cost-efficient, in order to meet the high growth of the wind power industry.

A. *Advances in the technical design*

Virtualizing controllers, repositories, and security functions through NFV, provides new opportunities to chain the virtual entities in workflows, and instantiating them dynamically on commercial off-the-shelf servers. Such level of elasticity will allow the composition, provisioning, and control of new services, to be done remotely and with reduced cost. NFV will also enable dynamic definition of slices [8] in the Wind Park for various tenants (users or applications) with different QoS needs, such as technicians upgrading device firmware and the turbine control applications. Complementary to the NFV, SDN will be used to dynamically create, provision, and operate paths for IP control and data flows, internal to the Wind Park, at the expected level of QoS. Services will be able to register their flow characteristics directly with the SDN controller. We foresee connection of the Wind Park to the remote control centre to be still over the Internet, where SDN allow the path to be setup and provisioned dynamically among the inter-connected network operators.

B. *Economic impacts*

The contribution of VirtuWind lies not only in a design of novel technological solution, but also includes a whole techno-economic framework to study the business feasibility of the proposed solution.

The number of Wind Parks installed and projects under development is growing with a tremendous pace. European strategy for green energy "20-20-20" (refers to 20% CO2 emission reduction, 20% renewables share, 20% power consumption reduction) is adding the stimulus and incentives to encourage investments in renewable energy. Total capacity of the offshore wind power in Europe in 2014 was 8 GW, which is enough to cover 1% of total EU consumption [9]. Considering the number of planned Wind Park projects and their typically long lifetime of 20 to 30 years it is clear that embracement of flexible, cost-efficient, and future-proof, like SDN and NFV, communication technologies has a great potential of economic savings.

A common way to measure and compare the cost efficiency of the power generation sources is the Levelized Cost of Electricity (LCOE). It is measured in terms of the cost incurred per kWh of electricity generated, i.e. lifetime cost divided by the lifetime electricity production. Hence, LCOE is proportional to CAPEX and OPEX as well as to the operational and active production life of the power plant. Our primary study show savings of 1.6 Million Euros in CAPEX, 0.16 Million of Euros in OPEX and 1.2 Eur/MWh in LCOE for a typical Wind Park (25 years lifetime, operating at 80 MW) [10].

Moreover, Careful scheduling of the upgrades and regular maintenance of the Wind Park should lead to longer operational time. Also, better predictability of the failures and more efficient failover mechanisms will ensure minimum downtime for unplanned interventions.

III. INDUSTRY NETWORK REQUIREMENTS

In order to identify requirements in the industrial networks, here we outline set of network configurations. These requirements are studied in the context of intra-domain network, inter-domain network, control and management, virtualization and network security. The intra-domain refers to the requirements that needs to be met within the network domain of the Wind Park. The inter-domain address such requirements when services needs to pass through domains of multiple operators while meeting stringent QoS requirements through the end-to-end (e2e) path. Figure 2 illustrates the requirements mapped to the Wind Park architecture.

Intra-domain network: within the single Wind Park domain, supporting broad variety of open and flexible interfaces that can enable network programmability is of significant importance. Hence, there is a need for new interfaces to allow applications and services requesting a data path inside the network domain with a certain performance. Therefore,

[4] Transmission Protocols - Network Access for IEC 60870-5-101 Using Standard Transport Profiles, IEC Standard 60870-5-104, 2006.

[5] MODBUS Application Protocol Specification v1.1b3, Modbus Organization Inc., 2012.

network monitoring, path computation and path instantiation entities are required.

Inter-domain network: the inter-domain network connects several network domains in order to establish an e2e data path with a specific performance. The VirtuWind architecture should support a heterogeneous inter-domain network environment since each network operator domain may apply different transmission technologies. Hence, new interfaces and mechanisms to request e2e connectivity with a given performance are needed. In addition, a (centralized or de-centralized) network entity is required to compute the e2e path fulfilling the requested performance. In this regard, monitoring and status information should be provided by different network operator domains as input to the path computation entities. Instantiating data path inside network operator domains and exchanging information among all involved entities require further considerations and unified interfaces.

Control and management: gathering information from the entire network, and keeping a detailed status for all forwarding devices, including their capabilities, load and reliability is another essential part of the VirtuWind network architecture. Such an entity will act as control/management and e.g. can calculate suitable data path that satisfy specific business application requirements.

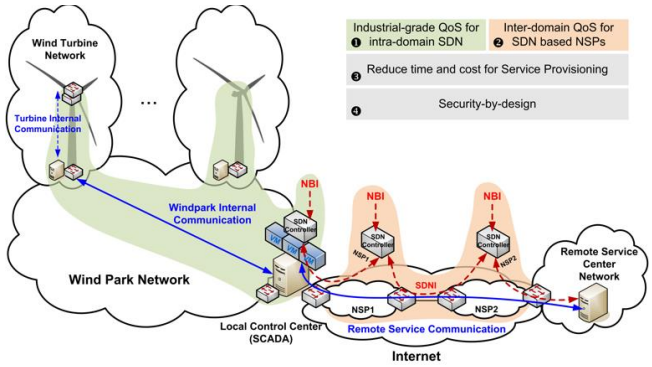

Figure 2: VirtuWind Requirements

Virtualization: an NFV infrastructure (NFVI) is required to manage the virtual appliances' environment [11]. The virtual appliances delivered as software only entities, such as data historian, virtual Router, and virtual Firewall, should be installed in and run in the local control centre, i.e. SCADA, to allow redundancy for critical components of the Wind Park.

Security: the nature of software increasingly used in SDN and NFV environments comes with additional security threats, such as data forging, API, controller and management exploitation need to be avoided by means of suitable mechanisms, e.g. strong authentication, access control, application isolation and sandboxing, flow integrity and conflict resolution as well as threat detection and encrypted interfaces.

In summary, proper path/track management is fundamental, with differentiated services capabilities including prioritisation of traffic flows and control plane signalling. The inter-domain space is also orchestrated by ability to manage resources across network boundaries, this is based in enabling traffic flows to ensure that the Service Level Agreements (SLAs) are met.

IV. NETWORK CHALLENGES IN THE WIND PARK

Despite being capital intensive, wind energy is still one of the most promising renewable technologies. The future of wind energy, however, will depend on the ability of the industry to continue to achieve cost reductions and, ultimately, to achieve cost parity with conventional sources of generation. Fluctuations in power output or frequency can have destabilising impact on the connecting grid so grid operators may be forced to disconnect the Wind Park from grid under extreme abnormal operating conditions. Such events have substantial impact on the levelized cost of wind park energy. Coordination of active and reactive power as well as the power frequency is not a one-time process, and thus requires reliable and delay-bounded set-point modifications during Wind Park's uptime. Variations of the external factors, such as the changing wind intensity and direction, energy market saturation and other grid events, affect the set-point values fluctuations that SCADA has to apply on individual wind turbines. The centralized SCADA should also be able to reliably shut down turbines in case of excessive or misbehaving production values. However, applying set-point values in deterministic and reliable way necessitates network infrastructure configuration that can ensure the strict QoS requirements. Control traffic flows are just examples of QoS-constrained network services in the wind park. Security camera services, secure remote access to turbine controllers or on-site video support are other types of network services, with relaxed delay requirements on one side, but with high bandwidth and availability demands on the other.

The centralized approach to network service embedding should enable on-demand admission and enforcement of a wide range of network services on the same physical substrate. The applications are assumed to hold very different combinations of QoS requirements, including those on, bandwidth guarantees, maximum end-to-end delay (latency), bit error rate and packet loss probability, availability and reliability, and service ranking and importance. All such QoS requirements should be addressed in the VirtuWind system-level design.

V. SYSTEM-LEVEL DESIGN

A. Realization of industrial-grade QoS for intra-domain SDN solutions

An important goal here is to ensure different stakeholders' needs, coming from their application requirements on network QoS and security, are being met at all times. The concept of network services should address necessary resource reservations and proper isolation of the application traffic. Supporting the embedding of different contending services on the same physical substrate will require sophisticated routing and resource allocation schemes to achieve these requirements. Furthermore, the following particular aspects of these requirements being addressed in the inter-domain network are foreseen:

Bandwidth guarantees: The intensity of the data transfer and burstiness characteristics will vary for different applications. Dynamic allocation of minimum bandwidth shares, which

considers the awareness of physical resources, should help in achieving optimal distribution of network resources ultimately maximizing the number of commissionable contending network services.

Maximum end-to-end delay: Primarily necessary in global coordination of WTGs to smoothen the frequency and voltage curves of output power and thus adhere to grid requirements. Today, SCADA-to-WTG set point update cycle times are typically at ~150ms, but are expected to be lowered by factor ten in the coming years.

Bit error rate and packet loss probability: Path provisioning will take into account the reliability of communication channels (noise, interference, distortion, bit synchronization errors, congestion etc.) and investigate utilization of redundant links to address unreliable links.

Availability and reliability: The feasibility of different strategies for ensuring highly available network service and correct delivery of critical applications' packets (e.g. considering redundant paths, packet duplication and duplicate-removal) in flexible network topologies will be investigated.

Service ranking and importance: Priority considerations will express the importance of different types of network services. This may be helpful in situations where multiple stakeholders or applications may compete for shared network resources.

To address the above, VirtuWind intra-domain design is based on dynamic embedding of traffic flows with flexible QoS guarantees at different levels of granularity, i.e. per-flow, per-application, and per-tenant.

Our initial design for per-flow dynamic QoS management, employ SDN controller and adjust the priority queuing throughout the path within a single domain for meeting QoS. Results from this initial prototype confirms that delay in establishing per-flow path through standard SDN controller should be shortened so as to address the industry-grade requirements [12].

B. Guarantee inter-domain QoS for multi-operator ecosystem

Providing guaranteed and stringent QoS across multiple domains needs yet another extremely robust design. Currently static SLAs between network operators are employed to assure that traffic traversing boundaries of each operator meets the defined QoS metrics. This implies a rigid and inflexible process which does not allow for dynamic and on-demand configuration of the underlying networks. Real-time interaction and negotiation between the controllers of multiple SDN-enabled operator domains will enable the establishment of high-QoS end-to-end paths. Also, it will allow the remote management over public Internet and reduce maintenance cost.

To achieve this, the SDN controllers of the involved domains expose an interface towards business applications to receive traffic characteristics. The SDN controllers negotiate application requested parameters and feasibility in their internal domains and eventually configure their underlying network infrastructure, especially their border SDN switches. This end-to-end negotiation considers each domain's internal policies and latest network capabilities, without exposing sensitive business information to the third parties (Figure 3).

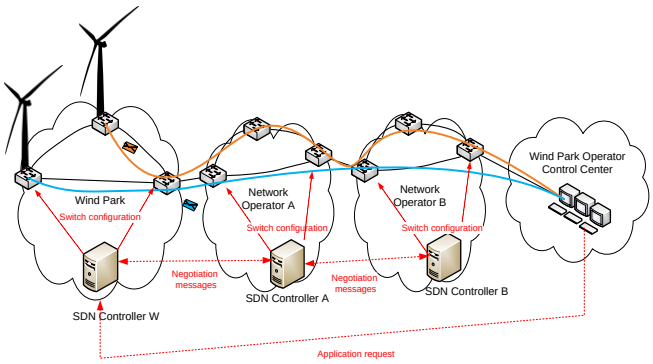

Figure 3: Inter-domain QoS negotiation

After successful negotiation, each SDN controller applies its internal traffic differentiation mechanism and marks application traffic flows accordingly, in order to setup high-QoS inter-domain paths. Configured switches are periodically monitored to ensure that application requirements are continuously met and capture links' failures which might require additional negotiation and path configuration.

Two different implementations of the inter-domain QoS negotiation are foreseen: (a) the *orchestrator-based* and (b) the *hop-by-hop* approach. In the first case all involved domains agree to participate and provide information of the paths and links to a centralized entity, called Orchestrator. Using this information, orchestrator receives the application requests, orchestrates the negotiation between domains, and configures the end-to-end inter-domain path.

In the hop-by-hop approach, the negotiation between SDN controllers is executed in a distributed fashion. Each domain checks its internal resources, selects and negotiates with the best next-hop domain without exposing any sensitive data and configures its SDN switches, until the destination domain is reached. Our primary protocol design for hop-by-hop QoS negotiation show that a lightweight protocol that employs SDN controller can negotiate QoS with a small overhead that is negligible for most business applications [13].

C. Reduction in time and cost for service provisioning and network maintenance

The current wind power plant network consists of network components with distributed control. There are different stakeholders for such a power plant, including Wind Park operator, grid operator, Wind Park owner and third party vendor. They all need customized access to their respective assets, which means the access for a particular service will either have limited time duration or constrained number of devices or have constrained industrial-grade QoS requirements or any of those combinations. As of today, providing customized access to different stakeholders of the SCADA communication network in a Wind Park is considered as labour- and time-intensive work. This is particularly true during Installation & Commissioning as well as during scheduled/unscheduled Operations & Maintenance activities.

To this end, SDN will bring programmability to the industrial network, thus increasing the velocity of service provisioning and reconfiguration, with substantial reductions in

OPEX. The cost for offering access to different stakeholders with different service profiles in the Wind Park network will also be significantly lower. Further savings are anticipated in CAPEX due to the cost reductions by using off the shelves hardware. These benefits are summarized in Figure 4.

D. Assurance of security-by-design

Introducing revolutionary concepts like SDN and NFV for critical infrastructures requires a careful investigation of the new security risks, since threats occur which have not been relevant in legacy systems. VirtuWind network needs to ensure the "security by design" concept for SDN including confidentiality, integrity, and availability of information, authentication, and non-repudiation and develops intra-domain proactive and reactive security mechanisms of the proposed framework. Thus, protection of the industrial cyber-physical system from external attacks, and also preventing that QoS requirements of industrial systems cannot be compromised by soft-failures.

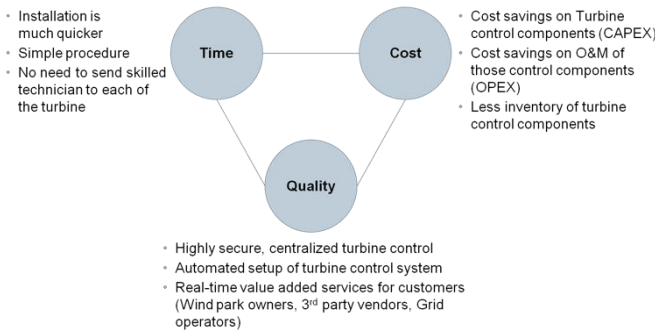

Figure 4: Time-Cost-Quality benefits of VirtuWind

The SDN infrastructure will be reachable from beyond a network services platform's domain and thus needs to be protected from misuse and abuse. More precisely, security mechanisms for the protection of controller and inter-controller interfaces should be established. In addition, mechanisms for ensuring accountability of controller actions affecting cyber-physical systems will be enabled. North bound interfaces (those interfaces to the business applications) should allow applications to express their requirements in terms of network policies, e.g. flow isolation, and QoS profiles. Based on the information exchanged through this interface, authentication and authorization of stakeholders could be realized via access and role-based lists for different levels of function granularities.

One of the core security mechanisms to be deployed in VirtuWind is network monitoring and intrusion detection for real-time identification of attacks and run-time network adaptation for attack response and mitigation mechanisms. The intrusion detection mechanism is based on 'honeypot' technology able to visualize and show in real-time the attacks in the inter-domain SDN. Trace-backs and audits enhancing root cause analysis during incident response, and failure analysis mechanisms can be established. We will also develop inter-domain incident detection and response security mechanisms. Such mechanisms will necessarily have to be 'reactive' and respond to situations and incidents as they arise. A framework for threat levels and incident reasoning will be defined and techniques for threat analysis and monitoring based on statistical techniques and learning will be deployed. The result will be an inter-domain incident detection component that will gather data from different layers and perform analysis based on machine learning techniques.

E. Virtualization and Multi-tenancy

Today, devices are tightly coupled to specific hardware which are currently expensive to scale and typically requires huge core switches with thousands of ports [14]. Some approaches suggested new complex protocols to be implemented on device hardware [15] or may confine merely with specific features such as IP-in-IP de-capsulation [16] and MAC-in-MAC encapsulations [15]. In essence they require huge forwarding table for storing MAC address of each VM. As a result, it significantly increases OPEX and CAPEX cost, complexity and security vulnerability.

In order to overcome the challenges (stated above), VirtuWind architecture supports virtualization and multi-tenancy to achieve large scale at low cost, with easy operation and configuration of substantial amount of VMs in addition with full isolation (what one tenant does should not affect any other) at reduced time and cost. Virtualization and multi-tenancy in VirtuWind particularly aim to move-off traditional Wind Park proprietary devices (e.g. data historian, firewall, router, honeypot) into virtualised environment inside a SCADA whereby these devices (now virtualised functions) will be controlled by an SDN controller and holistically managed by NFV Management and Orchestration (ETSI MANO) [11]. This will ensure industrial required QoS parameters, guaranteed on demand bandwidth and provide interoperability among vendors and operators of their virtualised products and infrastructure. Moreover, VirtuWind will augment existing ETSI orchestrator [11] to integrate legacy non SDN-enabled network devices with single common orchestrator.

VI. SUMMARY

This paper presents the vision and technical design concept of the VirtuWind project. This design is largely based on virtualization and softwarization in the industry control network by deploying SDN and NFV technologies. Industry networks are characterized with stringent QoS requirements while being mission critical and in need of extra security and reliability measures. Therefore, the design outcome of VirtuWind will address guaranteed industrial-grade security and QoS for intra-domain and inter-domain networks. In addition to the technical advances, we also show the significant economic impact of such open and flexible solutions.

ACKNOWLEDGMENT - THIS WORK HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 671648 (VIRTUWIND).

REFERENCES

[1] Open Networking Foundation. SDN Architecture Overview, 2013.

[2] S. Jain, et. al, "B4: Experience with a Globally-Deployed Software Defined WAN", *In Proc. SIGCOMM*, Aug. 2013, Hong Kong.

[3] T. Mahmoodi and S. Seetharaman, "Traffic jam: Handling the increasing volume of mobile data traffic," *IEEE Vehicular Technology*, No. 3, Vol. 9, pp. 56–62, 2014

[4] K. Jang, et. al., "Silo: Predictable Message Latency in the Cloud", *SIGCOMM Computer Communication Review*, No. 4, Vol. 45, pp. 435-448, 2015.

[5] M. P. Grosvenor, et. al., Queues don't matter when you can JUMP them!", *In Proc. NSDI*, May 2015, Oakland, CA.

[6] J. W. Guck ; W. Kellerer, "Achieving end-to-end real-time Quality of Service with Software Defined Networking", *In Proc. IEEE CloudNet*, Oct. 2014, Luxembourg.

[7] M. Condolucci, et. al., "Softwarization and Virtualization in 5G Networks for Smart Cities", *In Proc. Int'l Conf. on Cyber physical systems, IoT and sensors Networks (CYCLONE)*, Rome, Oct. 2015.

[8] M. Jiang, et. al., "Network slicing management & prioritization in 5G mobile systems", *In Proc. European Wireless*, May 2016, Oulu.

[9] EWEA, A The European Offshore Wind Industry: Key Trends and Statistics 1st Half 2015

[10] VirtuWind deliverable, "Design of Techno-economic framework", *D2.4*, Oct. 2016, available online: www.virtuwind.eu.

[11] ETSI white paper, "Network Function Virtualisation (NFV)", Oct. 2013.

[12] F. Sardis, et. all. "Can QoS be dynamically manipulated by the end-device initialization", *In Proc. IEEE ICC workshops*, Kuala Lampur, May 2016.

[13] G. Petropoulos, et. al., "Software-Defined Inter-networking: Enabling Coordinated QoS Control Across the Internet", *In Proc. Int'l. Conf. on Telecommunications (ICT)*, Thessaloniki, May 2016.

[14] M. Arregoces and M. Portolani. Data Center Fundamentals. *Cisco Press*, 2003.

[15] C. Kim, M. Caesar, and J. Rexford, " Floodless in SEATTLE: A Scalable Ethernet Architecture for Large Enterprises", *In Proc. SIGCOMM*, Seatle, Aug. 2008, Seatle, WA

[16] A. Greenberg, J. Hamilton, and N. Jain, " VL2: A Scalable and Flexible Data Center Network", *In Proc. SIGCOMM*, Aug. 2009, Barcelona.