Incentives for a Softwarization of Wind Park Communication Networks

Petra Vizarreta, Amaury Van Bemten, Ermin Sakic, Khawar Abbasi, Nikolaos E. Petroulakis, Wolfgang Kellerer, and Carmen Mas Machuca

Wind energy is one of the most attractive and one of the fastest growing sources of green energy in the world. With the expansion of wind parks, there is a growing need for an efficient coordination of the diverse energy production systems, as well as a tighter coupling between the production and the consumer side of the grid.

Abstract

Wind energy is one of the most attractive and one of the fastest growing sources of green energy in the world. With the expansion of wind parks, there is a growing need for an efficient coordination of the diverse energy production systems, as well as a tighter coupling between the production and the consumer side of the grid. Current grid operators have unnecessarily high costs due to the lack of an integrated management system toward a diverse set of proprietary network protocols, complex and error prone operation of the networks, as well as rigid security mechanisms. Network softwarization concepts, that is, SDN and NFV, offer great potential for reducing capital and operational expenditures by providing simplified network management and automated control. Recent works have demonstrated the feasibility of achieving stringent industrial-grade quality of service and fine grain security control with SDN and NFV. In this article, we provide an insight into wind park communication network requirements, analyze the technological benefits of the network softwarization, and demonstrate the economic profits in a case study of a typical Northwestern Europe wind park.

Introduction

Wind energy is one of the most affordable and fastest growing sources of renewable energy, with more than 500 GW of installed capacity worldwide in the past 20 years. Incentives from national governments, as well as the ones proposed through the Renewable Energy Directive by the European Commission targeting at covering 20 percent of energy needs with renewables by 2020, further promote the widespread adoption of green power plants. As the number of installed wind parks is rapidly increasing, there is a need for their tighter coupling and the efficient coordination of energy production schedules [1]. Smart Grids, which are considered a promising solution for the integration of a diverse set of energy production and distribution systems, require deep penetration of ICT technologies in all of its subsystems. However, current wind parks are not yet prepared for a seamless integration into the Smart Grids, mainly due to the lack of mechanisms for the automated and secure exchange of information [2].

Industrial communication networks, such as the one in wind parks that in the past have been developed as closed systems, rely on closed proprietary protocol stacks, which have been tailored and optimized for their particular requirements. Different Industrial Ethernet protocols were developed to accommodate the stringent industrial-grade requirements for latency, jitter and reliability, necessary to provide the stable operation of power control networks. The lack of compatibility between different Industrial Ethernet protocols leads to vendor lock-in, since wind park owners must deploy components from the same manufacturer to ensure their interoperability. Furthermore, existing wind park communication networks suffer from high configuration and management complexity. Network upgrades and updates are error prone and time consuming as they require customized scripting tools and many hours of testing performed by highly specialized network engineers. Also, network maintenance and failure reparation are costly and incur a loss of revenues due to a reduction of power production, as wind turbine generators need to be taken out of service during the maintenance operations. Moreover, security breaches, such as Ukraine's power plant hack in 2015, are not uncommon, despite the deployment of sophisticated network security appliances. The exposure to cyber-attacks is only expected to increase in the context of Smart Grids [3].

The 5G concepts of network softwarization, that is, Software Defined Networking (SDN) and Network Function Virtualization (NFV), have shown to be a promising solution to solve several practical issues regarding protocol openness and fine grained security control, as well as the full automation of network configuration and management [2]. With SDN, the distributed control plane logic of forwarding devices, that is, switches and routers, is moved to a software entity called the SDN controller. The SDN controller provides an integrated interface toward the forwarding devices, which significantly simplifies network management and augments network programmability. Providing standardized and open interfaces toward network components helps network operators avoid vendor lock-in, and hence to obtain lower prices through an increase in market competitiveness. In NFV higher-layer network devices, such as firewalls or intrusion detection systems, which are traditionally implemented in specialized hardware, are replaced with modular software components deployed on commodity hardware. Such modular network functions can be further

Digital Object Identifier:
10.1109/MCOM.2019.1800492

Petra Vizarreta, Amaury Van Bemten, Wolfgang Kellerer, and Carmen Mas Machuca are with the Technical University of Munich; Ermin Sakic is with Siemens AG; Abbasi Khawar is with Intel Shannon; Nikolaos E. Petroulakis is with the Foundation for Research and Technology Hellas.

0163-6804/19/$25.00 © 2019 IEEE

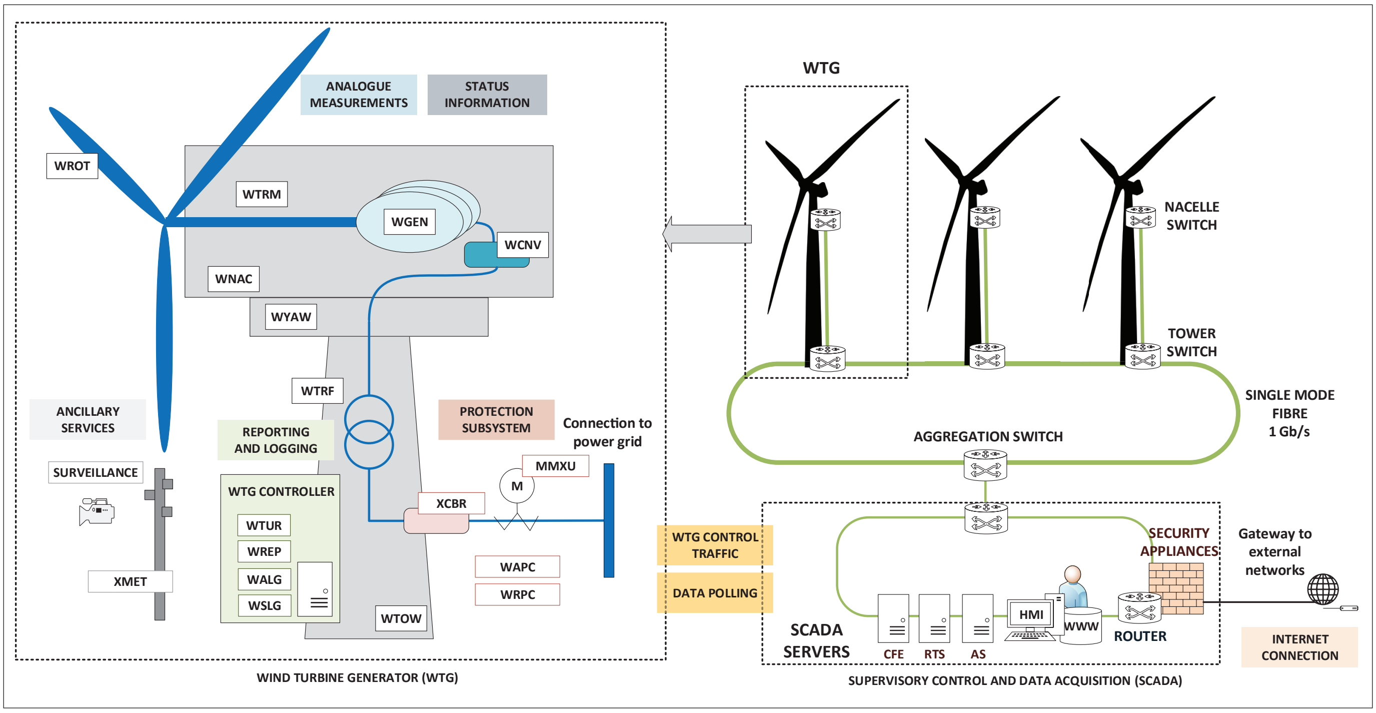

Figure 1. Inside the wind park communication network.

chained to provide fine grained traffic control, offering much greater flexibility and lower cost of service deployment for wind park network owners and industrial network operators in general.

First studies on software-defined industrial networks have shown that it is possible to achieve deterministic delay [4], high availability and low recovery times [5, 6], and guarantee high security standards [7] with commodity SDN switches and general purpose hardware. The feasibility of achieving industrial grade quality of service with an open and extensible protocol suite provided by state-of-the-art SDN and NFV solutions has already been demonstrated in an operational wind park environment as a part of the VirtuWind project [2]. Our goal in this article is to discuss and explore the technological and economic incentives for wind park owners and operators to softwarize their networks. Due to the limited size of the wind park which is not representative of typical wind parks, we considered parameters of typical off-shore wind parks in Northwestern Europe.

The remainder of the article is organized as follows. The following section presents an overview of existing wind park communication networks. We then describe the technological and economic benefits of communication network softwarization. The economic advantages are then evaluated on a typical wind park in Northwestern Europe. The final section concludes the article with a summary of the main findings presented in this article.

Wind Park Communication Networks

In this section we first present the different classes of traffic in wind park communication networks, and the requirements imposed on the underlying networks in terms of data rate, latency, reliability and packet loss. Then we present the design and limitations of the existing wind park communication networks.

Traffic Classes

The principal communication actors in the wind park are located in wind turbine generators (WTG) and Supervisory Control and Data Acquisition (SCADA) system, as illustrated in Fig. 1.

Wind Turbine Generators (WTGs): Wind turbine generators represent a complex system of intelligent electronic devices (IEDs) and remote terminal units (RTUs) that consist of sensors, actuators and an internal controller. According to the international standard IEC 61400-25 "Communications for monitoring and control of wind power plants" [8], which provides a framework for information exchange within a wind park, IEDs and RTUs in WTGs are grouped into logical nodes based on their function, as shown in Fig. 1. Every logical node supports three classes of traffic: status information, analogue measurements and control information. For instance, a wind turbine rotor (WROT) sends *status information* regarding the rotor and the blades, *analogue measurements* of the rotor speed and the temperature, and receives the *control information* to set the pitch angle for the blades or set the rotor to a blocked position. As part of the substation automation, each WTG must be equipped with multiple IEDs or RTUs, such as measurement merging units and circuit breakers, providing *protection switching* control against overcurrent and overvoltage. The role of the *reporting and logging system* is to provide full traceability of the sequence of events in case of a failure. It provides information derived from the original measurements and status messages. Reports are provided on demand, while log files are transmitted periodically to the SCADA. *Video surveillance* is used for security, to detect the ships or vehicles that are approaching the wind park, as well as to monitor the state of the turbines and the environment. Video can be streamed continuously or requested on demand.

Service	Direction	Priority	Data rate	Latency	Reliability	Packet loss rate
Protection traffic	WTG → SCADA	1	76,816 bytes/s	4 ms	99.999%	$< 10^{-9}$
Analogue measurements	WTG → SCADA	2	225,544 bytes/s	16 ms	99.99%	$< 10^{-6}$
Status information	WTG → SCADA	2	58 bytes/s	16 ms	99.99%	$< 10^{-6}$
Reporting and logging	WTG → SCADA	3	15 KB every 10 minutes	1 s	99.99%	$< 10^{-6}$
Video surveillance	WTG → SCADA	4	250 kb/s – 1.5 Mb/s	1 s	99%	No specific requirement
Control traffic	SCADA → WTG	1	20 kb/s per turbine	16 ms	99.999%	$< 10^{-9}$
Data polling	SCADA → WTG	2	100 bytes every 2 ms 2 KB every second	16 ms	99.99%	$< 10^{-6}$
Internet connection	Internet → WTG/SCADA	3	1 GB every two months	60 min	99%	No specific requirement

Table 1. Traffic classes and services present in the wind park. The consolidated QoS requirements are based on the relevant industry standards [8–10] and previous case studies on wind park [11–13] and SCADA [14] architectures.

Supervisory Control and Data Acquisition (SCADA): A typical SCADA system consists of several application servers, as shown in Fig. 1. The communication front end (CFE) server is used for data acquisition from field devices (RTUs and IEDs), and can also perform protocol conversion and temporary storage of measurements and status data for real-time data trending. Real time servers (RTS) are in charge of data processing, real-time operational process control and short-term data trending, while the archive servers (ASs) are used for long term data storage. The system also has a human machine interface (HMI) to facilitate user interaction with the network and to allow engineers to access and modify the operational data, and display alarms and power plant status information. The web server (WWW) provides a user interface to the SCADA via a web interface for the users who access the system via their personal computer.

The traffic from the SCADA toward the wind turbines consists of two components: constant *control traffic* and *periodic data polling*. *Internet access* and interfaces to third party systems are also provided. This includes internal interfaces to meteorological mast and video surveillance, as well as external interfaces to the Internet, national grid and other control centers, according to IEC 60870 [9] and IEEE C37.1-2007 [10].

The traffic classes and their QoS requirements are summarized in Table 1. The consolidated QoS requirements are based on the relevant industry standards [8–10] and the previous case studies on wind park [11–13] and SCADA [14] architectures.

Communication Network

The communication system in the wind park is designed to guarantee the industrial-grade requirements of the services specified in Table 1, required for a reliable flow of control and monitoring traffic between the SCADA and WTGs. WTGs are typically grouped in rings and radials to maximize energy production. The topology of the communication system is constrained to the layout of the power collection system, since optical fibres that interconnect turbines and the SCADA are embedded in the power line cables. A typical power cable has up to four optical fibres, which support 1:1 protection and also offer huge capacity to support bandwidth hungry applications, such as video surveillance. The links within a turbine are either optical fibres or twisted pairs.

As depicted in Fig. 1, there are typically two access switches in each wind turbine: one at the top that is distributing the traffic between sensors and actuators of IEDs and RTUs, wind turbine controller and other ancillary functions; and one at the bottom that is handling the traffic between turbines and the SCADA. Core switches aggregate the traffic coming from different radials. Unfortunately, standard Ethernet switches do not provide guaranteed latency since the queuing delay is not bounded. Hence, special switches, implementing Industrial Ethernet protocols are required to ensure deterministic delay. The ecosystem of switches capable of supporting wind park requirements is rather small. Ensuring inter-compatibility forces wind park operators to deploy all network components from the same vendor, such as *Connected Grid* and *Industrial Ethernet* switches by Cisco, or complete network solutions provided by major wind turbine vendors.

The router and the gateway in the SCADA enable communication with external networks. Typical wind park routers, such as *Cisco 2000 Connected Grid Router*, support VLANs with IPSec, which are usually deployed to isolate different traffic classes and to limit the access to sensitive control traffic only to authorized users.

Security is of the paramount importance in industrial networks. Advanced security appliances, such as the ones provided by the *Cisco ASA 5000* Series, are comprised of firewall, intrusion detection and prevention system and deep packet inspection functions. Security appliances in legacy wind parks are deployed as software bundles running on the specialized proprietary hardware, which is a setup typically optimized for high volume traffic in data centers and enterprise networks. This approach incurs unnecessarily high cost for wind park operators. Security breaches are not uncommon, despite the sophisticated mechanisms deployed in the power plants, calling for the design of new security solutions that are tuned better for industrial purposes, as shown in the next section.

Technological Incentives

Next, we introduce the architecture of a softwarized wind park and discuss how SDN and NFV can be used to solve the practical issues regarding

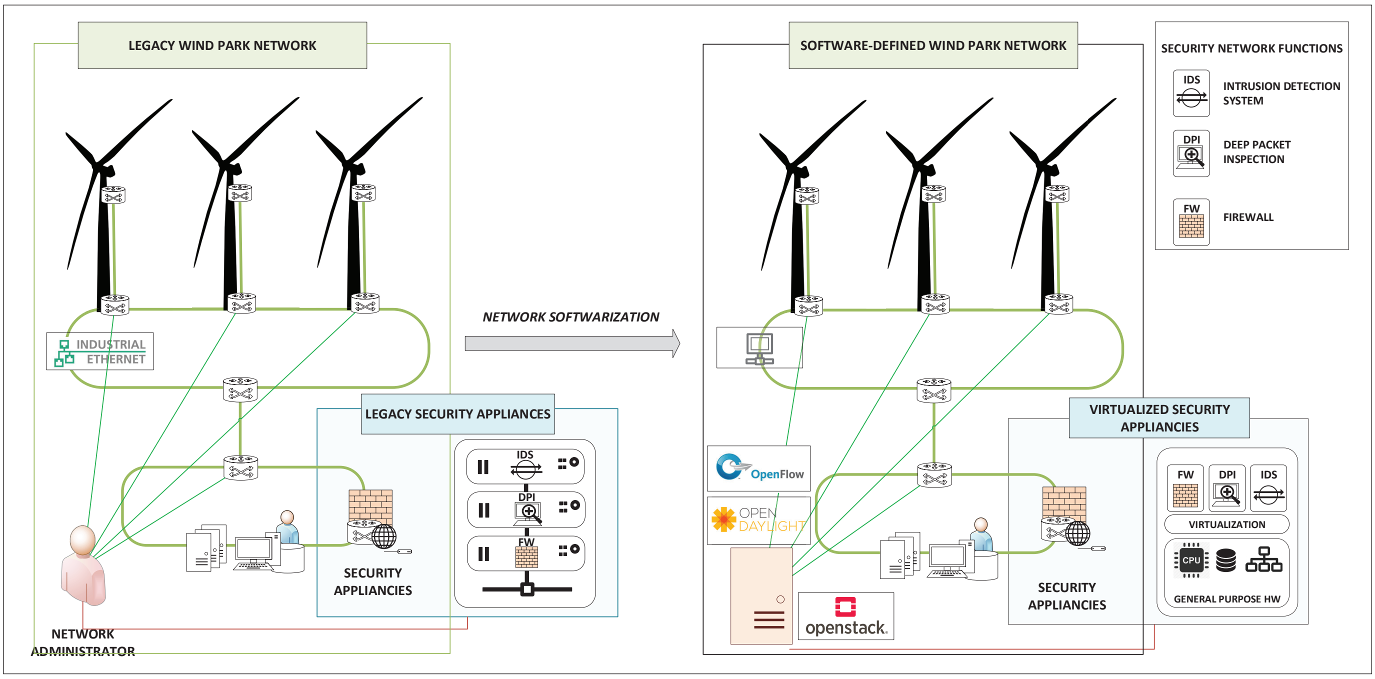

Figure 2. Technological incentives for softwarization: A) SDN: replacing proprietary Industrial Ethernet switches with programmable commodity switches for an efficient network management. B) NFV: replacing monolithic security appliances, with modular virtual network functions for a fine-grained security control.

protocol openness, the fine grained security control and highly automated network management.

SDN: Replacing Industrial Ethernet with Programmable Switches

In legacy wind parks, the industrial grade of service (e.g., deterministic latency) is guaranteed with a closed protocol suite based on Industrial Ethernet, since standard Ethernet switches cannot provide bounded queuing delays. In SDN, the switch control plane logic is outsourced to the SDN controller. The controller has a global overview of the network state, and can provide delay guarantees through logically centralized queue-level flow management [3, 4], as illustrated in Fig. 2.

SDN-enabled switches are simpler, and hence cheaper than Industrial Ethernet switches, and the price gap is expected to increase as the technology matures. Already today, there is a myriad of high-end commercial switches already deployed in enterprise and data center networks, from white box solutions (e.g., EdgeCore AS4610 with Pica8) to big networking hardware vendors (e.g., HPE FlexFabric 5930 and Aruba 3800), offered at a competitive price. Moreover, commodity SDN-enabled switches support standard Ethernet, facilitating the seamless integration of different energy production systems, without the need for protocol converters.

The SDN controller provides high-level network abstraction and vendor agnostic management. This allows users and applications to specify high level intents, such as the opening of a new TCP port at the set of firewalls or the setup of a connection between two hosts with a specified quality of service, without minding the low level forwarding rules that need to be configured in the switches. The SDN controller can program the forwarding plane with OpenFlow, an open and standardized protocol managed by the Open Networking Foundation (ONF).

A centrally managed programmable forwarding plane significantly simplifies the setup of new services, since the configuration scripts do not have to be customized for a specific network equipment vendor. Vendor agnostic network control and management are expected to reduce the need for a specialized team of technicians. The automation of network configuration is also expected to reduce the incidence of human errors. Open source SDN controllers, such as OpenDaylight, already provide support for most commercial switches.

NFV: Virtualization of Security Network Functions

The most complex network components in wind parks are security appliances, embedding the functionality of firewall, intrusion detection and prevention system and deep packet inspection. Due to the small size of the market for industrial security solutions, wind park operators typically deploy solutions developed and optimized for enterprise and data center networks. With NFV, specific security functions can be realized as modular software components running on general purpose hardware, replacing the monolithic security appliances implemented in specialized proprietary hardware, as illustrated in Fig. 2. Such a setup offers resource pooling, as well as a high degree of flexibility when choosing the preferred vendor for the particular security module.

A prototype of an NFV-based solution for industrial networks, based on open source firewall (pfSense), IDS (Snort), deep packet inspection (nDPI) and customized honeypots (HoneyD) was presented in [7]. These modular software components, which are often packaged as virtual machines, can be further chained to provide fine grained security control. For instance, unknown traffic flows are first processed and classified by DPI, while trusted SCADA traffic can bypass it to avoid unnecessary delays. Malicious traffic is redirected to honeypots

Network component	Network components in legacy wind parks			SDN/NFV vs. legacy network components		
	Cost [€]	Power [W]	MTBF [h]	Cost [%]	Power [%]	Failure rate [%]
Access switches	3.330	40	263.285	78	75	65
Aggregation switches	2.324	100	203.812	87	95	65
Router and gateway	2.490	210	289.056	85	67	90
Security appliances	3.674	90	299.588	88	133	90

Table 2. Comparison of the network components in legacy wind park and SDN/NFV based network. The reference values for cost, power consumption and Mean Time Between Failures (MTBF) represent the median of the available commercial products from different vendors. Provided figures are based on publicly available price lists, as well as data sheets provided by major wind turbine vendors and Cisco solution for industrial networks (legacy components), EdgeCore, Pica8, HPE, Aruba and Dell (SDN/NFV components).

that emulate a wind park network, in order to distract attackers and allow the operator to collect valuable data about the ongoing attack.

In legacy networks the customized configuration scripting tools and highly specialized network engineers are required for operation and maintenance of security appliances. On the other hand, NFV offers complete automation of management and orchestration (MANO) of network functions. The reference architectural framework and MANO interfaces are specified by the ETSI NFV group. Several open source solutions, such as Open Source MANO (OSM), already provide solutions for the management of shared physical network infrastructure, virtualization layer and service function chaining.

Impact on Network Design

The architectural changes introduced by SDN and NFV are illustrated in Fig. 2. With SDN Industrial Ethernet switches are replaced by OpenFlow enabled switches, while with NFV monolithic security appliances are replaced by software modules running on general purpose hardware. The comparison of commercial network components in legacy and SDN/NFV based wind parks is presented in Table 2. The network functions implemented in software require additional general purpose servers. The cost of the servers can be divided between all the software components proportionally to their utilization of physical resources (CPU, RAM, storage). The licensing of the software depends on the business model of the particular vendor in the case of commercial network solutions, while for open source solutions software development and maintenance are provided by the community. Open source network control and management platforms, such as OpenDaylight supported by the Linux Foundation, have already shown stable performance in commercial network deployments.

Economic Incentives

In this section we address the economic incentives for wind park softwarization. First, we present the cost models for capital and operational expenditures to quantify the savings that can be achieved by the softwarization of a wind park communication network. We illustrate the magnitude of savings in the case study of a typical offshore wind park in Northwestern Europe.

Cost Factors

Capital Expenditures (CAPEX): CAPEX include all the costs related to the network equipment, including supporting infrastructure and installation cost. Since the focus of our analysis is to evaluate the cost differences between legacy and SDN/NFV based communication networks, this study considers the cost of (i) access switches in WTGs, (ii) aggregation switches, (iii) router and gateway and (iv) security appliances. We also consider the cost of the additional blade servers that need to be installed in order to support software based network components.

$$CapEx = \sum_{\forall comp\, i} N_i Price_i$$

The number of network components (N_i) that need to be purchased during the lifetime of the wind park depends on several parameters used by network planning such as the component's capacity, the desired redundancy level, and estimated lifetime and vendor warranty period. The traffic volume in wind parks is relatively low (Table 1), and active redundancy is typically deployed only in the SCADA. An expected wind park lifetime (T_{oper}) is 20 to 30 years, while the typical lifetime of network components is five to 10 years.

Operational Expenditures (OPEX): OPEX include all the costs associated with operation and maintenance activities incurred during the lifetime of a wind park communication network. The most important ones are configuration ($Config_{cost}$), power consumption ($Power_{cost}$), preventive maintenance ($Maint_{cost}$), corrective maintenance or failure reparation ($FailRep_{cost}$) and cost of energy not supplied (CENS).

$$OpEx = Config_{cost} + Power_{cost} + Maint_{cost} + FailRep_{cost} + CENS$$

Configuration Cost: Any adjustment of the network, such as the opening of a TCP port or the addition of a new sensor to the wind park network, requires the reconfiguration of network components that has to be performed during the maintenance window, which occurs N_{main} times per year. A team of highly specialized network engineers needs T_{config} man-hours to write and test the configuration scripts. It has been demonstrated that configuration time is significantly reduced in SDN/NFV based networks, thanks to the high degree of automation and vendor agnostic management provided by the SDN controller and NFV MANO. The hourly cost of the network engineers is w_{nw}.

Power Consumption: Given a power cost *PC*, the power consumption cost can be directly computed as the sum of the power consumption of all active network components. It can be seen in Table 2 that, while the power consumption of SDN switches and routers is slightly lower than the power consumption of their legacy counterparts, the power consumption of virtualized security appliances running on commodity hardware is actually higher.

Preventive Maintenance: Network equipment needs regular maintenance to guarantee acceptable operational conditions as a part of proactive failure management. Inspection of the network equipment

Wind park parameters		Country specific parameters		Network specific parameters	
Operational time	$T_{oper} = 20$ years	Power consumption	$PC = 0.28$ €/kWh	Maint. window	$N_{main} = 4$ times/year
Number of turbines	$N_{WT} = 80$	Cost of technician	$w_{tech} = 58$ €/h	Configuration effort	$T_{config} = 8$ man-hours (legacy) $T^{*}_{config} = 15$ minutes (SDN/NFV)
Power rating	$WT_{rating} = 4$ MW	Cost of nw. engineer	$w_{nw} = 52$ €/h		
Capacity factor	$CF = 40\%$	Transport to SCADA	$Trav_{scada} = 100$ €	Maintenance effort	$T_{main} = 8$ man-hours (legacy) $T^{*}_{main} = 30$ minutes (SDN/NFV)
Travel time to turbines	$T_{wt} = 24$ h	Transport to turbines	$Trav_{wt} = 1000$ €		
Interruption time	$IT = 120$ h	Power penalty	$PP = 150$ €/MWh	Aggregation factor	$AG = 8$ turbine/radial

Table 3. Case study: typical offshore wind park in north-west Europe. Wind park parameters are based on the publicly available data, country specific data are based on the data from [15], and network specific data are based on data gathered from EU OASE and VirtuWind projects.

is performed N_{main} times a year and it requires a team of technicians for T_{main} man-hours. Maintenance activities, such as switch firmware upgrades, are expected to be faster and simplified in softwarized networks since they can be mostly done remotely. The hourly cost of the technicians is w_{tech}.

In softwarized networks, the network functions implemented in software also require regular maintenance, in terms of feature upgrades and security updates. Primarily the control and management functions, that is, the SDN controller and NFV MANO, need to be updated regularly. Note that our network solution relies on open source components maintained by the community. We have shown in our previous work that open source SDN controllers reach the stable phase after four months [6]. Even in the case of commercial solutions, the cost of software development, testing and debugging can be shared between all deployed wind parks.

Failure Reparation: The expected number of failures of a network component during its operational lifecycle can be derived from MTBF values provided by the vendors. The repair cost of a single failure depends on the hourly cost of the technicians (w_{tech}) and the time required to repair the failure $MTTR_i$, as well as the cost of their transportation to the site, either SCADA ($Trav_{scada}$) or wind turbine ($Trav_{wt}$). Note that in the case of offshore wind parks, the time to reach the wind turbine (T_{wt}) is a dominating factor, and $T_{wt} \gg MTTR_i$, since a boat or a helicopter may be required for the transportation of technicians. Previous case studies have shown that most network outages in legacy wind parks are related to switch port failures. Most of the failures are caused by human error, which is not accounted for in the *MTBF* values shown in Table 2. Since the operation of SDN switches involves minimum human intervention, the reduction of the failure rates, and consequently the cost of failure reparation, is expected to be even higher.

CENS: Wind turbine generators need to be taken out of operation during failure reparation. During the interruptions, wind park operators not only lose money that they could have earned by selling the harvested energy, but would also have to pay penalties to the grid operator for not supplying the promised quantity of energy. Given a power penalty *PP* per interrupted MWh, expected interruption time *IT*, a wind turbine power rating (production capacity) WT_{rating} and its capacity factor (efficiency of power production) of *CF*, the expected CENS can be evaluated. Note that the interruption time (*IT*) is larger than the failure reparation time $IT \gg MTTR_i + T_{wt}$ since it also includes failure detection, diagnosis, procurement of the equipment and team preparation.

Case Study

The total cost of the ownership of a wind park depends on a number of factors such as the type of project (e.g., number and location of turbines), country specific parameters (e.g., cost of technicians and engineers) and network design parameters (e.g., aggregation factor). In order to illustrate the magnitude of savings due to network softwarization, we present the case study of the typical offshore wind park in Northwestern Europe. The relevant case study parameters are summarized in Table 3.

The contribution of the individual CAPEX and OPEX cost factors is presented in Fig. 3. Significant savings can be observed in both CAPEX and OPEX. More than 442,000€, that is, 19.85 percent, of savings can be achieved in CAPEX thanks to the lower cost of softwarized network components. OPEX reduction is expected to be even higher, around 34 percent, accounting for more than 1,380,000€ accumulated savings during the lifetime of the wind park.

The reduction of the cost of the access switches in the wind turbine contributes most to the CAPEX savings. The highest cost reduction in OPEX is expected from CENS, due to the shorter interruptions of power production. The second biggest contribution to the OPEX savings comes from failure reparation, due to the significantly lower failure rates.

Provided that some of the baseline scenario parameters have high uncertainty, as well as the fluctuations due to the regional differences, we conducted the local sensitivity analysis to estimate the impact of individual factors on the total savings. As expected, the number of turbines and the lifetime of the wind park have the highest impact, since it influences all cost components. The factors driving CENS (*CF*, *PP*, *IT*, WT_{rating}) and failure reparation (w_{tech}, $Trav_{wt}$) also have a significant impact.

We also assess the impact of the wind park size on the expected savings. We observe that in large wind parks with more than 300 wind turbines (e.g., the Hornsea in the U.K. has 342 turbines), the total savings are estimated to be more than 7 Mil. €. The relative savings, however, do not change significantly with respect the wind park size, and it converges to 20 percent of CAPEX and 35 percent of OPEX savings in communication network cost.

In softwarized networks, the network functions implemented in software also require regular maintenance, in terms of feature upgrades and security updates. Primarily the control and management functions, that is, SDN controller and NFV MANO, have to be updated regularly.

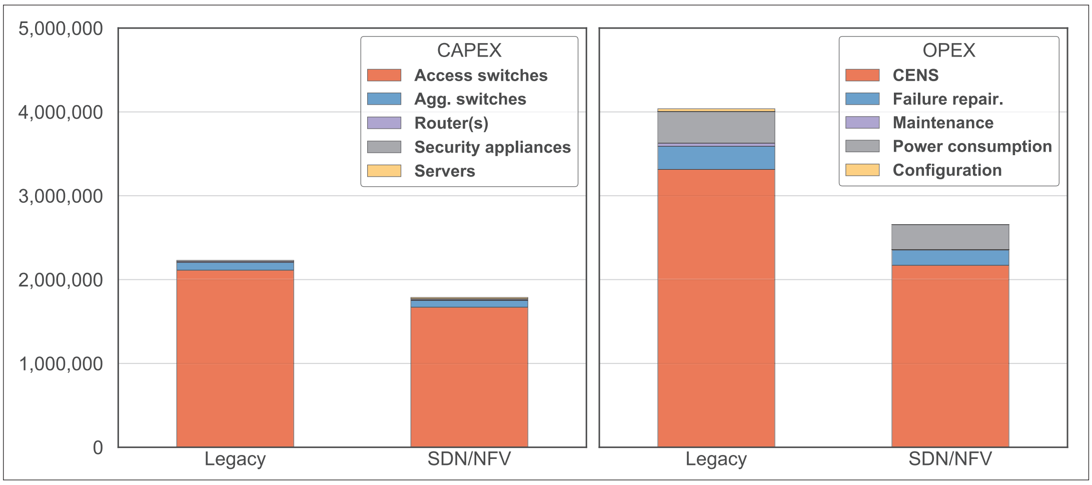

Figure 3. Analysis of economic incentives for softwarization of the wind park: 19 percent of the savings in CAPEX and 34 percent in OPEX can be expected.

Conclusion

In this article, we have presented a study of the techno-economic feasibility of the softwarization of wind park communication networks. Software Defined Networking (SDN) and Network Function Virtualization (NFV) are introduced to solve the limitations of legacy wind parks by providing the protocol openness and the fine grained security control necessary for the tighter integration of wind parks into future Smart Grids. Capital and operational expenditures have been modeled in order to quantitatively evaluate the benefits of SDN and NFV. A case study of a typical wind park in Northwestern Europe has demonstrated that significant savings can be achieved through network softwarization, making it a promising solution to facilitate its seamless integration into Smart Grids. The advantages of network softwarization in wind parks trigger new open questions for operators such as the identification of seamless migration paths while guaranteeing simultaneous park operation.

References

[1] K. Wang *et al.*, "Green Energy Scheduling for Demand Side Management in the Smart Grid," *IEEE Trans. Green Commun. and Networking*, vol. 2, no. 2, 2018, pp. 596–611.

[2] T. Mahmoodi *et al.*, "VirtuWind: Virtual and Programmable Industrial Network Prototype Deployed in Operational Wind Park," *Trans. Emerging Telecommunications Technologies*, vol. 27, no. 9, 2016, pp. 1281–88.

[3] Cyber-Attack Against Ukrainian Critical Infrastructure. ICS-CERT, Alert (IR-ALERT-H-16-056-01), 2015.

[4] J. W. Guck, A. Van Bemten, and W. Kellerer, "DetServ: Network Calculus Models for Real-Time QoS Provisioning in SDN-Based Industrial Environments," *IEEE Trans. Network and Service Management*, 2017.

[5] E. Sakic and W. Kellerer, "Response Time and Availability Study of RAFT Consensus in Distributed SDN Control Plane," *IEEE Trans. Network and Service Management*, vol. 15, no.1, 2018, pp. 1932–4537.

[6] P. Vizarreta *et al.*, "Assessing the Maturity of SDN Controllers with Software Reliability Growth Models," *IEEE Trans. Network and Service Management*, vol. 15, no. 3, 2018, pp. 1090–1104.

[7] K. Fysarakis *et al.*, "A Reactive Security Framework for Operational Wind Parks Using Service Function Chaining," *IEEE Symposium on Computers and Commun.*, 2017, pp. 663–68.

[8] International Electrotechnical Commission, IEC, "International standard 61400-25: Communications for monitoring and control of wind power plants."

[9] IEEE Standard 1646-2004, "Communication Delivery Time Performance Requirements for Electric Power Substation Automation."

[10] IEEE Standard C37.1-2007, "Supervisory Control and Data Acquisition (SCADA) and Automation Systems."

[11] S. Thilo, "The Three Generations of Field-Level Networks—Evolution and Compatibility Issues," *IEEE Trans. Industrial Electronics*, 2010, pp. 3585–95.

[12] M. A. Ahmed and Y. C. Kim, "Network Modeling and Simulation of Wind Power Farm with Switched Gigabit Ethernet," *International Symposium on Communications and Information Technologies (ISCIT)*, 2012, pp. 1009–14.

[13] M. Wei, Z. Chen, and S. Member, "Study of LANs Access Technologies in Wind Power System," *IEEE PES General Meeting*, 2010, pp. 1–6.

[14] A. L. Pettener, "SCADA and Communication Networks for Large Scale Offshore Wind Power Systems," *IET Conf. Renewable Power Generation*, 2011.

[15] M. Forzati *et al.*, "Next-Generation Optical Access Seamless Evolution: Concluding Results of the European FP7 Project OASE," *J. Optical Communications and Networking*, vol. 7, no. 2, 2015, pp. 109–23.

Biographies

Petra Vizarreta [S'19] is a research associate at the Chair of Communication Networks of the Technical University of Munich (TUM), where she is currently pursuing the Ph.D. degree. Her research interests include modeling and design of dependable softwarized networks, and their applications in industrial networks.

Amaury Van Bemten [S'18] is a research associate at the Chair of Communication Networks at TUM, where he is currently pursuing the Ph.D. degree. His current research focuses on routing algorithms and the application of software-defined networking for real-time communications in industrial environments.

Ermin Sakic [S'17] is a research scientist at Siemens AG. He is pursuing the Ph.D. degree with the Chair of Communication Networks at TUM. His research interests include reliable and scalable Software Defined Networks, distributed systems and efficient network and service management.

Abbasi Khawar is a Technical Lead with NPG at Intel Shannon, Ireland. His experience includes cloud orchestration (NFV, SDN, and OpenStack), and routing and switching and now leading Intel's Resource Director Technology (RDT).

Nikolaos E. Petroulakis is a research scientist at the Foundation for Research and Technology Hellas (FORTH). His Ph.D. is on network security from City University of London.

Wolfgang Kellerer [M'96, SM'11] is a full professor with TUM, heading the Chair of Communication Networks. He currently serves as an associate editor for *IEEE Transactions on Network and Service Management* and on the editorial board of *IEEE Communications Surveys and Tutorials.*

Carmen Mas Machuca [M'96, SM'12] is privat dozent/adjunct teaching professor at the Chair of Communication Networks, TUM. Her main research interests are in the area of converged access networks, techno-economic studies, network planning and resilience, and SDN/NFV optimization problems.