Building a testing environment for SDN networks analysis for electrical grid applications

Toni Cantero-Gubert[†]
Power Systems Group
IREC
Sant Adrià de Besòs,
Barcelona, Spain
tcantero@irec.cat

Alba Colet
Power Systems Group
IREC
Sant Adrià de Besòs,
Barcelona, Spain
acolet@irec.cat

Pol Paradell
Power Systems Group
IREC
Sant Adrià de Besòs,
Barcelona, Spain
pparadell@irec.cat

J.L. Domínguez-García
Power Systems Group
IREC
Sant Adrià de Besòs,
Barcelona, Spain
jldominguez@irec.cat

ABSTRACT

Cyberattacks are becoming a serious thread for power systems; its prevention is gaining attention and needs to be better understood by developers, technology providers and network operators among others. In order to gain knowledge on such risks, and due to the fact that power systems are critical infrastructures, there is the need to have laboratories that allow developing such tests without putting at risk the energy service. To this aim, such laboratory must include two flexible networks (i.e. communications and electrical) which are completely integrated and allow to identify the impact of one into the other. In this paper, a testing platform developed by IREC for programmable communication networks integrated into electrical microgrids is presented. Such integrated lab-testing platform is aimed to meet the requirements of smart grids in terms of intelligent control, communications, monitoring and self-healing techniques as well to allow testing cybersecurity developments.

CCS CONCEPTS

• General and reference → Cross-computing tools and techniques → Evaluation; Measurement; Experimentation

KEYWORDS

Cybersecurity, Software-Defined Networking (SDN), microgrid, programmable network, resilience, laboratory, experimental setup, hardware-in-the loop (HIL)

ACM Reference format:

Toni Cantero-Gubert, Alba Colet, Pol Paradell, and J.L. Domínguez-García.2020. Building a testing environment for SDN networks analysis for electrical grid applications. In The 15th International Conference on Availability, Re-liability and Security (ARES 2020), August 25–28, 2020, Virtual Event, Ireland. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3407023.3409230

https://doi.org/10.1145/3407023.3409230

1 INTRODUCTION

The electric sector is in continuous process of evolution; the trends are in line of increase the electrification, modernize the power system and distribute the generation, so new challenges needs to be addressed to guarantee the security it requires as a critical infrastructure in our society. This change is led by the disruption and rapid spread of digitalization technologies as technologies of information and communication (TIC), cloud computing, Internet of Things (IoT) sensors and many others that has provoked the evolution of the classic distribution grid to the Smart Grid. The digitalization of the electrical grid is necessary to meet the requirements of smart grids in terms of intelligent control, communication, monitoring and self-healing techniques [1].

The digitalization of electrical grid brings many advantages but also exposes those installations to new threads unknown for the electrical systems; such as information leak or alteration for a misuse. The potential consequence of those threads could destabilize the electric grid and create a blackout, with fatal consequences to the infrastructure and to the society. [2]

In this regard, there is the need to make the grid more resilient in order to minimize the impact of any of that potential risks or attacks. By taking advantage of increased flexibility, provided by distributed generation, energy storage system, electric vehicles, self-consumption systems, among other, it is possible to increase network resilience by the use and creation of microgrids which can operate both grid-connected and islanded. Such potential islanding capacity helps ensuring the customer service even during such electrical network disruptions. From the cybersecurity and Smart Grid point of view, it is relevant to consider the communication network interlinked with the electrical grid, since both networks are strongly related. Focusing on this, there is one new concept that is attracting interests as the Software-Defined Networking (SDN). It is a network architecture approach that enables the network to be intelligently and centrally controlled using software applications. In other words, SDN concept allow to have pre-defined strategies in case of networking problems, leading to increase resilience and security, since the system will react faster than traditional networks.

In this paper, it is presented a testing platform for programmable networks integrated in microgrids with the aim to meet the requirements of smart grids in terms of intelligent control, communication, monitoring and self-healing techniques. Two contributions have been made: 1) It is established a network communication between monitoring and metering equipment commonly present in power system through an SDN-based architecture with virtual elements in order to test complex topologies and with physical equipment to check the Quality of Service (QoS) of the communication. 2) It is created a hardware-in-the loop platform between a grid emulator that acts as a node of a distribution network simulated in a real-time equipment. The grid emulator feeds a microgrid with the ability of work in islanded mode in case of cyber-physical attacks to the distribution grid infrastructure.

2 WHAT IS SDN?

SDN stands for software-defined networking. It provides programmable access to the network devices, allowing a communication network to detect and react to failures and congestions at run time. SDN is based on open protocols, such as OpenFlow, to apply globally aware software control at the edges of the network to access network switches and routers that typically would use closed and proprietary firmware. In addition, it enables the network to be intelligently and centrally controlled using software applications. All these features can conceptually be represented as the separation in 3 planes: The data plane consist on the network switches and elements that forward data obeying the rules set by the controller, the control plane acts as the brain of the architecture deciding the processing paths and other functions to control the network switches. Finally, the application plane consist on programs that communicate specific needs to the controller building intelligence intro the communication network without the need to deal with network infrastructure (Figure 1).

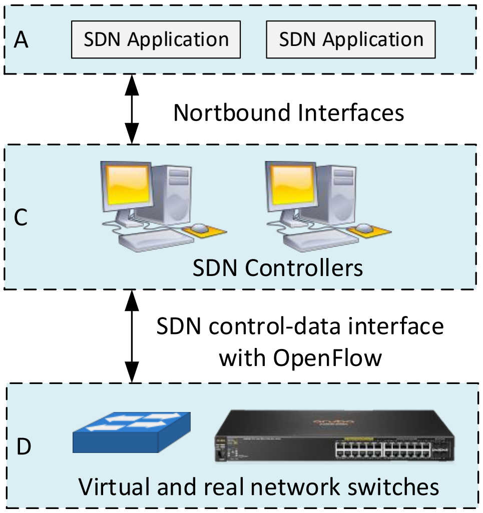

Figure 1: SDN architecture conceptualized in planes: (A)pplication plane, (C)control plane and (D)ata plane

SDN can be used to create applications to analyse and achieve diverse QoS requirements. In this regard, the implementation of SDN in microgrids is of relevance to increase system security and resiliency since it exploits programmable network to enhance communications. Furthermore, it helps operators manage the entire network consistently and holistically, regardless of the underlying network technology [3].

Such research field is gaining attention in the last years and few projects are dealing with its application and implementation into electrical power systems such as SPEAR or SDN-microSENSE. SDN-microSENSE aims at providing and demonstrating a secure, resilient to cyber-attacks, privacy-enabled, and protected against data breaches solution for decentralized Electrical Power and Energy Systems (EPES). All designed, developed, and tested technologies should consider the latest related research findings and maintain high compliance with current industrial standards (e.g., IEC standards) [4].

2.1 Benefits of using SDN in microgrids

The incorporation of SDN into microgrids can offer some great advantages over conventional networks: The traditional hardware-dependant communication infrastructure is not designed to identify the flow and context of the data and it only focuses on packet forwarding using pre-defined network configurations. SDN provides programmability, dynamicity, flexibility, and intelligence to current network architectures, and its benefits can be delivered from four main features: dynamic flow control, network-wide visibility with centralized control, network programmability and simplified data plane [5]. The data flows can be entirely controlled from the main controller and protection paths can be defined in advance, so in case of a failure the system behaves in a predicable way [6]. The rearrangement of the network in a microgrid can be used to eliminate unnecessary network traffic, prioritize the data flows of critical assets and to isolate the compromised nodes in case of an attack [7]. Furthermore, SDN provides some benefits in the microgrid architectures managed by a central controller, allowing not only managing field devices but also monitoring and controlling the network that interconnects system devices. It also adds more flexibility to the central controller by easily adding new field devices or upgrading existing network applications. A better integration of geographically disperse network equipment from different versions could be done by using a standardized protocol such as Open Flow. Finally, a range of customized services, e.g., to perform load balancing between communication links, to optimize the operation of system components, or even to identify and mitigate traffic anomalies, could be created [8].

While SDN-based communication infrastructure provides many benefits, SDN may also introduce resilience and security issues. For instance, the controller can become a single point of failure, the communication between the network switches and the SDN controller may lead to latencies, SDN controller may contain software vulnerabilities and may be subject to cyber-attacks. SDN is evolving and solutions are found: Use multiple SDN controllers to balance the load, use backup rules installed proactively in the network switches, so they can react directly without involving the SDN controller. [9]

A resilient communication infrastructure with flexible QoS support is indispensable to accomplish the requirements for the data used in the emergency control of microgrids. In those conditions, the microgrid is in the risk of rapid changes that may cause instability and eventually a collapse in the system. The combination of electric power with SDN networks, to understand the state of the power network in real-time and to tests the advantages of such technology, is a challenge and requires from tests beds to co-simulate network and power systems [10].

3 TESTING PLATFORM

The facilities of the Catalonian Institute for Energy Research (IREC) count with the Energy Smart Laboratory (SMARTLAB) that has a configurable AC three-phase network, which interconnects several power electronics converters, battery storage systems, power load banks, commercial self-consumption kits, emulated devices and virtual devices simulated with real-time equipment. It allows for real physical equipment to operate under a broad range of scenarios being suitable for experimental validations [11]. A centralized SCADA is used to monitor all the components and experiments through a dedicated communication infrastructure. To explore the feasibility and effectiveness of the SDN-based communication architecture for microgrids, a testing platform is built using a broad number of devices present in the laboratory.

3.1 Equipment description

The involved devices used in the design of this platform have been classified in two main groups of elements depending if they belong to the electric or the communication network:

1) The power electronics system (Figure 2):

- A 200 kVA grid emulator that acts as voltage source setting up the reference voltage and frequency of the emulated microgrid. It represents a MV to LV substation in the electric power system.
- An emulated distribution line consisting on a variable inductance and a resistance that range from 0 to 20 Ohms both the resistance and the reactance. Its parameters can be adjusted depending on whether it is need to represent a strong or weak grid.
- A bunch of load/generator emulators with 4-kVA maximum apparent power operation that will be the equipment that represent the consumers or the distributed generation in the microgrid.
- A *BYD* LV lithium-ion battery with an energy capacity of 11.5 kWh.
- Three *Sunny Island 6.0h SMA* inverters with 6 kW nominal power each, prepared to work in cluster and provide a 3-phase voltage source when the microgrid requires working in islanded mode.
- The automatic transfer switch, i.e., the device prepared to disconnect the voltage source created by the grid emulator from the microgrid, in case of fault in the supply. This device will reconnect the microgrid to the grid emulator when the fault is solved and the control operator allows it.
- An *OPAL-RT* equipment that will allow real-time hardware-in-the-loop (HIL) simulation of the electric system. It will simulate a complete grid behaviour while interacting with the grid emulator as the real equipment of the electric grid.

2) The control and communications system (Figure 3):

- A Schneider Electric Remote Terminal Unit (RTU) connected to the grid emulator provides electric measurements to a centralized system. It represents a typical measurement unit present in an electrical substation, it can communicate with different protocols and it will be connected to the SCADA.
- A Supervisory Control and Data Acquisition (SCADA) where the experiments are controlled and the information gathered.
- An *Aruba* network switch (JL255A) that supports multiple programmable interfaces, including REST APIs and Openflow 1.0 and 1.3, to enable automation of network operations, monitoring, and troubleshooting. The bandwidth for each port is 1 Gbps.
- A *Raspberry Pi 4* development board that comes with Gigabit Ethernet where a virtual SDN topology is created.
- A computer with *Mininet* 2.3, *Open vSwitch* 2.9.1 and a *Ryu* controller 4.30 with Ubuntu 14.04 operating system working as the SDN controller.

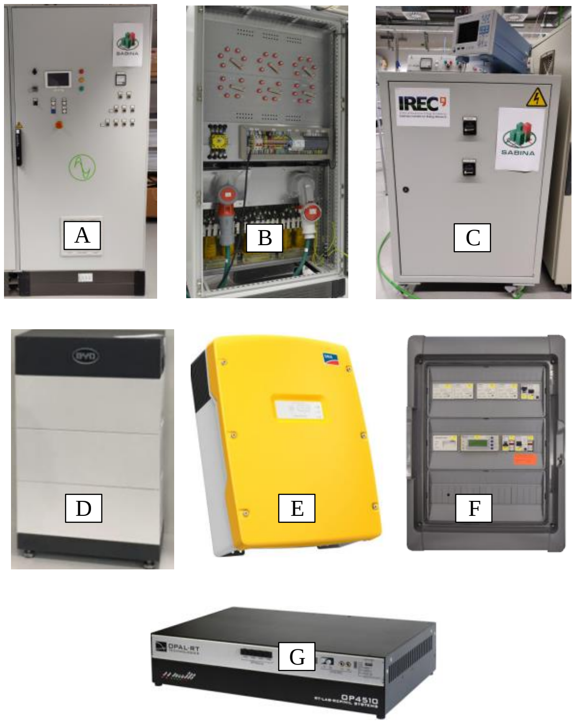

Figure 2: Some of the components of the power electronics systems, A) Grid emulator, B) Line emulator, C) Emulated load/generator, D) *BYD* LV lithium-ion battery, E) *SMA Sunny Island* inverter, F) Automatic Transfer Switch distribution panel and G) *OPAL-RT* simulator

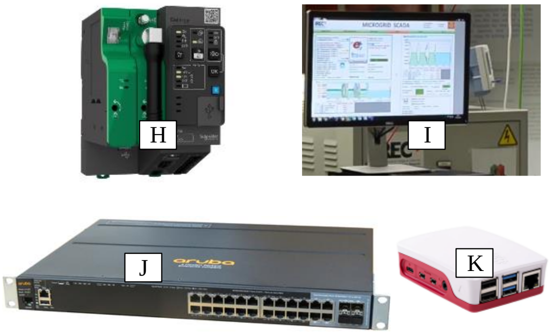

Figure 3: Some of the components of the control and communication system, H) *Schneider Electric* RTU, I) SCADA, J) *Aruba* Network Switch, K) *Raspberry Pi* development board.

3.2 SDN-based communication architecture

The architecture of the SDN-based communication includes both a physical switch in order to deal with the QoS of real equipment and virtual switches so the network topology can be as extended as desired. This hybridization is an advantage to create complex topologies while checking its performance with physical equipment. The network contains a network switch that support OpenFlow, a Raspberry Pi with Mininet network emulator software and a laptop with the Ryu SDN controller running on it. Mininet is a software tool that allows the creation of virtual hosts, switches, controllers, and links; its switches support OpenFlow and it enables complex topology testing, without the need to wire up a physical network. The SDN controller runs on another dedicated computer, it is based on RYU, a component-based software defined networking framework, freely available under the Apache 2.0 license. The SDN controller communicates with the all the virtual and the physical switches using the OpenFlow protocol. The testbed used for this paper consist on 4 network switches (3 of them are virtual and they are emulated in the Raspberry Pi and the other is the *Aruba* network switch (Figure 4). The switches are forming two paths (each with 3 switches) between the electrical substation and the control centre. In the same communication channel, it will exist communication from the RTU to the SCADA to provide electric measurements and the other way around in case the SCADA request the RTU to implement some actions (trigger a digital output or consult the GPS signal, among others). The communication channel will be shared with the OPAL-RT that sends reference setpoints to the grid emulator, while this last one will provide power measurements to the simulated interface.

While in practice a network path may contain more switches than in our testbed, adding more switches on a path does not provide additional insights for the test cases. Using real hardware though it is important since it allows us to obtain realistic measurements. With this architecture, some functionalities can be monitored: Network latency, traffic prioritization, rerouting time in case of network failure or the dynamics of the electric supply response in case of power supply failure.

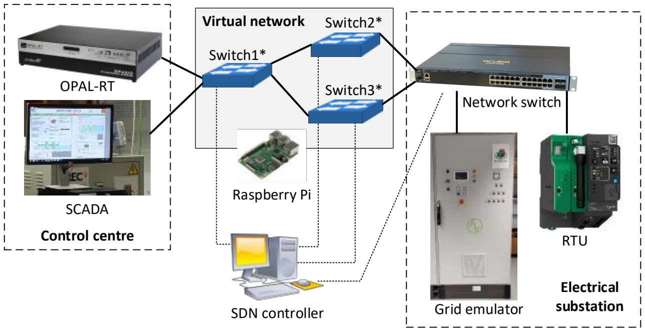

Figure 4: Network architecture with two paths available for the routing of the data between the electrical substation and the control centre. The SDN controller is physically connected to the network switch and the Raspberry Pi and virtually connected to Switch1*, Switch2* and Switch3*

3.3 Electrical grid closed-loop control

Modelling a real-world grid has been possible with the help of a Distributed System Operator (DSO) data. Its electrical network topology has been represented in the *OPAL-RT* by means of *Matlab-Simulink* computer software. The grid emulator present in the laboratory facility will act as a node of the entire network and its behaviour will be affected by the operation of the entire grid. The *OPAL-RT* will send the reference setpoints as the voltage and frequency to the grid emulator substation, which in turn will provide the measurements of active and reactive power consumed by the microgrid to the real-time simulator (Figure 5). The closed-loop control for the voltage and frequency falls into the real-time simulator.

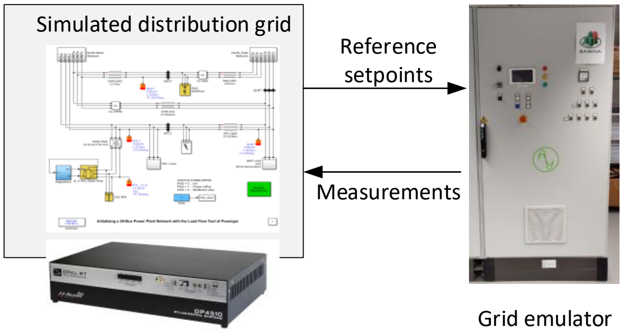

Figure 5: Closed-loop control of grid emulator setpoints

3.4 Power system deployment

The grid emulator, acting as an electrical substation is connected to the microgrid by means of a line emulator that allows the configuration of a strong or weak grid. The microgrid consist on several loads/generations representing different consumption or generation up to 4 kW each (Figure 6). In case of fault in the grid emulator, the microgrid will be supplied by the battery and inverters.

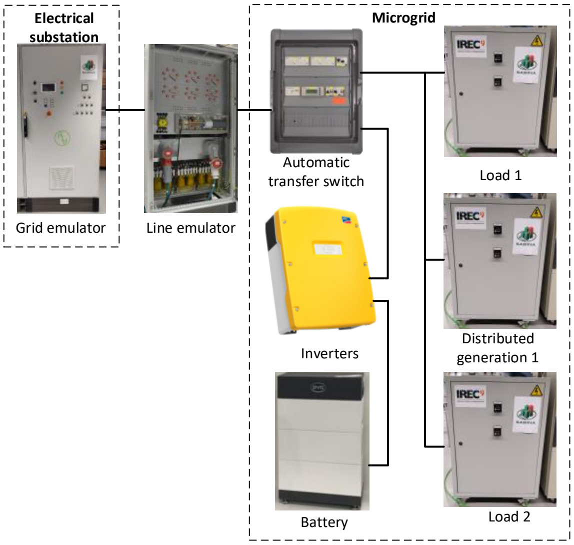

Figure 6: Simplified electric schematic of the power system used in the testing platform

4 TESTING METHODOLOGY

This testing platform allows exploring the feasibility and effectiveness of the SDN-based communication architecture for microgrids, it serves as well to evaluate the dynamics of the electrical power system compared with traditional communications. Two practical use cases are presented in this paper:

1) Rerouting in case of communication network failure: It will consist on the reaction of the testbed when one of the virtual switches (Switch2* or Switch3*) is disabled either by a physical or cyberattack. Since it still exists an alternative network path, the SDN controller should suggest a different routing for the affected data as fast as possible.

2) Microgrid emergency control: It will consist on the reaction of the laboratory equipment when the communication between the electrical substation and the control centre is lost or it has been an electrical fault so the microgrid is no longer electrically supplied by the grid emulator. In both cases, the microgrid has to be isolated from the grid emulator and powered by the battery and the inverter in islanded mode.

The indicators to evaluate the performance of the proposed communication architecture will be:

- Network latency [ms]: It is the total round-trip time from the data frames to cross the network from the electrical substation to the control centre in the different scenarios.
- Traffic prioritization [%]: Different priority data is travelling within the same network; it is studied the percentage of packets that need to be dropped to guarantee the high priority communication.
- Automatic rerouting [ms]: It is the total time it takes to restore the communication when a switch has failed and it exist other routing paths.
- Island reaction [ms]: It is the total time it takes the battery and inverters to supply a voltage reference to the microgrid when it has been an electric shutdown or a communication failure that cannot be restored immediately.

With the aim to ensure the reliability of the experimental setup deployed in the laboratory, the tests run for at least 3 day long. An electrical fault will be configured in the grid emulator and randomly triggered, as it would occur in real networks. The fault has to last as much as 2 hours while the distributed generation and the batteries are supplying the energy needs of the microgrid. An example for the second use case could be that two electrical faults are detected between 6h and 8h and between 18h and 20h during the same day (Figure 7).

4.1 Preliminary results

For the first case it is compared the SDN enabled self-healing to the traditional Spanning Tree Protocol (STP) for rerouting in case a switch is disabled and it exist other routing paths. The mechanism to compute the new path is by running Dijkstra's shortest path algorithm on the updated graph representation of the communication network. The self-healing mechanism utilized through the RYU platform is at the network layer focusing on host-to-host self-healing by selecting the shortest path. In addition, RYU supports multipath forwarding out of the box, which is an advantage over the STP protocol that must build loop free topologies. The path of the data packets (blue-green rectangle) can be seen using a network visualization tool (Figure 8).

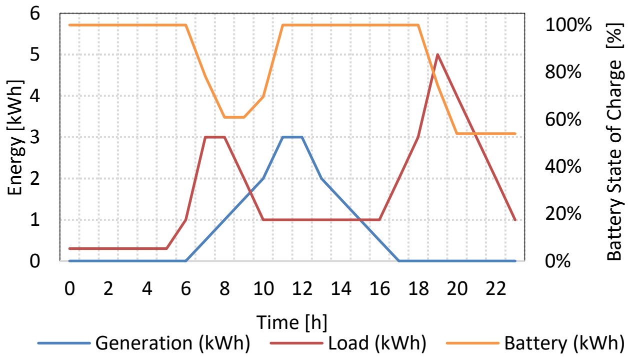

Figure 7: Energy generation and consumption per hour expected in the laboratory test for the microgrid emergency control

STP creates a spanning tree from a network graph and disables any links forming cycles. Messages are periodically exchanged, therefore when the topology changes, the network detects the change and converges to a new network configuration. This requires four missed messages and a listening and learning stage that takes 25 seconds or longer depending on network settings.

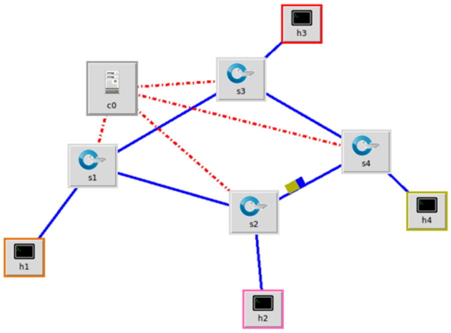

Figure 8: MiniNAM software visualization tool is used to see the changes on the data paths when a switch is attacked. In the figure the data packets are going from the switch S2 to the switch S4 when switch S3 is disabled.

4.2 Upcoming tests

Automatic rerouting, network latency times and traffic prioritization need to be calculated for the self-healing mechanism and compared with the STP protocol, as the complete tests have not been carried out.

The dynamics and stability of the microgrid and the island reaction time needs to be evaluated too in the upcoming tests.

5 CONCLUSIONS

This paper aimed to present the ongoing tasks and developments carried out in the field of cybersecurity in electrical power systems. The features of SDN-based architecture are highlighted and it is remarked the benefits it can bring to both the communication network and the electrical grid operation. In this regard, the SDN approach can help in the application and evolution of microgrid communication networks, facilitating the development of network applications and increasing system resilience.

In addition, the need of specific testing platforms has been arisen and justified. To answer such need, IREC has developed a testing platform allowing the integration, testing and validation of cyber-threads into a controlled electrical environment, as well as the application of SDN algorithms and technologies. Such testing environment will allow full testing of cyber-attacks and potential countermeasures into electrical equipment and communication devices. This is required to validate developed tools before using them in the real electric grid, which is a critical infrastructure.

As further work to be developed and implemented in such unique lab-testing infrastructure, the focus goes on: 1) A self-healing technique that will provide the optimal routing after an attack or a risk is detected in the communication infrastructure and 2) The transient responses from the electrical equipment when there is a fault in the electric supply of the microgrid. The system dynamics and stability will also be evaluated.

ACKNOWLEDGMENTS

The research leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833955.

REFERENCES

[1] G. Dileep (2020). A survey on smart grid technologies and applications. Elsevier Renewable Energy, 2589–2625.

[2] M. McGranaghan, M. Olearczyk and C. Gellings (2013). Enhancing Distribution Resilience: Opportunities for Applying Innovative Technologies. Electricity Today, vol.28, no 1, 46-48.

[3] K. Cabaj, J. Wytrębowicz, S. Kukliński, P. Radziszewski and K. T. Dinh (2014). SDN Architecture Impact on Network Security. Federated Conference on Computer Science and Information Systems, Warsaw, 2014.

[4] European Union’s Horizon 2020. https://www.sdnmicrosense.eu/

[5] S. Shin, L. Xu, S. Hong and G. Gu. Enhancing Network Security through Software Defined Networking (SDN). 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa, 2016.

[6] J. Kim, F. Filali and Y. B. Ko (2015). Trends and Potentials of the Smart Grid Infrastructure. MPDI Applied Sciences, vol. 5, p. 706-727.

[7] D. Jin, Z. Li, C. Hannon, C. Chen, J. Wang, M. Shahidehpour and C.W. Lee (2017). Toward a Cyber Resilient and Secure Microgrid Using Software-Defined Networking. IEEE Transactions on Smart Grid, vol. 8, no. 5, p. 2494-2504.

[8] M. A. Moyeen, F. Tang, D. Saha and I. Haque. SD-FAST: A Packet Rerouting Architecture in SDN. 15th International Conference on Network and Service Management, Halifax, 2019.

[9] L. Ren, Y. Qin, B. Wang, P. Zhang, P. B. Luh and R. Jin (2015). Enabling Resilient Microgrid through Programmable Network. IEEE Transactions on Smart Grid, p. 1-11.

[10] Z. Lu, C. Sun, J. Cheng, Y. Li, Y. Li and X. Wen (2017). SDN-Enabled Communication Network Framework for Energy Internet. Hindawi Journal of Computer Networks and Communication, vol. 2017, p. 1-13.

[11] M. Marzband, A. Sumper, A. Ruiz-Álvarez, J. L. Domínguez-García and B. Tomoiaga (2013). Experimental evaluation of a real time energy management system forstand-alone microgrids in day-ahead market. Applied Energy, p. 365–376.