Specifications of a Simulation Framework for Virtualized Intelligent Electronic Devices in Smart Grids covering Networking and Security Requirements

Nadine Kabbara
EDF, Utrecht University
Paris Saclay, France
nadine.kabbara@edf.fr

Agrippina Mwangi, Madeleine Gibescu
Utrecht University
Utrecht, Netherlands
{a.w.mwangi, m.gibescu}@uu.nl

Ali Abedi, Alexandru Stefanov, Peter Palensky
Delft University of Technology
Delft, Netherlands
{a.abedi-1, a.i.stefanov, p.palensky}@tudelft.nl

2023 IEEE Belgrade PowerTech | 978-1-6654-8778-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/POWERTECH55446.2023.10202950

***Abstract*—As power system's operational technology converges with innovative information and communication technologies, the need for extensive resilience testing for scenarios covering the electrical grid, networking bottlenecks, as well as cyber security threats, become a necessity. This paper proposes a comprehensive, multi-disciplinary simulation framework to test virtualized intelligent electronic devices (vIEDs), considering 1) functional requirements, 2) performance and quality of service of the underlying communication network using software-defined networking, and 3) cyber security intrusion detection schemes. This work serves as a reference for researchers interested in the grid modernization of information and communication infrastructure for future power systems. Six different cyber security attack surfaces have been identified within the framework scope. It was observed that migration of vIEDs due to device maintenance or external anomalies is interesting from an operational perspective yet still poses significant security threats. Therefore, both host-based and network-based intrusion detection schemes were analyzed. Also, the setup has been mapped to an offshore wind case study demonstrating its potential and possible scenarios to simulate.**

***Index Terms*—virtualized intelligent electronic devices, software-defined networking, intrusion detection, IT/OT, simulation framework, cyber-physical power systems**

I. Introduction

Electrical power grids are undergoing major transformations due to the rise of intermittent renewable energy, electrification of heat and transport sectors, and advances in information and communication technologies, which further add cyber security threats. A smart power grid is typically comprised of sub-components responsible for its overall operation and management. The sub-components include: (i) physical infrastructure assets - primary equipment, intelligent electronic devices (IEDs), sensors, and actuators; (ii) information layer - the functional logic operating the physical infrastructure; and (iii) the communication layer - connecting the equipment to assure inter-communications and remote connection to supervisory control and data acquisition (SCADA) systems.

The heterogeneous sub-layers require deploying complex, often dedicated information and communication technology (ICT) infrastructure. Operating this inflexible legacy infrastructure is subject to human errors and on-site interventions with added costs. In response, it is argued that grid modernization efforts in the area of protection, automation, and control infrastructure will help resolve these issues while meeting the requirements of a more resilient power system [1].

Current trends are moving towards improving operational technology (OT) efficiencies for future grids by leveraging best implementation practices from the information technology (IT) world (e.g., cloud, virtual machines, containers). Virtualization technology can be defined as 'software which emulates different hardware level functionalities and creates an equivalent *virtual* or *software-based* computing system' [2].

Virtualization has seen a multi-disciplinary adoption (IT, network function virtualization NFV and software-defined networking SDN, and more recently, part of Industry 4.0) thanks to its potential benefits. Notably, the benefits of virtualization include: (i) reducing operation and management costs (OPEX); (ii) reducing equipment costs (CAPEX) by replacing dedicated hardware with software-implemented functions; (iii) portability of virtual instances; (iv) optimizing productivity; and (v) disaster recovery support [3]. These advantages are of interest to the power system domain where a promising application concerns the management and operation of a fleet of IEDs [3].

However, providing the proper frameworks and testing tools for scenarios covering the electrical grid, networking bottlenecks, as well as cyber security threats will be necessary. Therefore, in this paper, we propose a simulation framework based on the concepts of virtual IEDs (vIED), their communication networks, and cyber security surfaces of attacks. This subject has been dealt with in several previous research.

Project Funding:
This paper has been developed under the umbrella of the InnoCyPES project (Innovative tools for cyber-physical energy systems). This research has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 956433.

A. State of the art

Several studies explore portable deployment technologies like virtual machines and containers to facilitate testing different networking and cyber security scenarios on OT power networks. For example, Hage Hassan et al. [1] use the virtualization of IEDs to mitigate network contingency problems. Similarly, De Din et al. [4] demonstrated the scalability of containerized distributed controllers for distribution automation. However, works by [1], [4] did not cover the potential of SDN within their frameworks. Rosch et al. [5] developed a setup based on SDN but only focused on testing containerized IEDs' latency performance.

As for cyber security, Ansari et al. [2] developed a virtualized remote terminal unit (RTU) testbed where a cyber attack on the device level was emulated. Also, Attarha et al. [6] analyze security problems of virtualized energy systems; However, functional interoperability and real-time performance were outside the work scopes of both [2], [6].

Therefore, it can be observed that previous works covered the concepts of OT grid modernization following a siloed domain test setup. The lack of a comprehensive framework for simulating vIEDs, advanced networking concepts (including SDN/NFV), and cyber-physical intrusion detection methods motivates our work. This novel framework allows testing various scenarios covering the multi-disciplinary solution's performance requirements and the specifications of the information exchange model for the involved power system actors.

B. Paper Contributions and Organization

The contributions of this paper are the following:

1) Proposal and specification of a comprehensive, multi-disciplinary simulation framework for vIEDs considering functional, networking, and cyber security requirements of smart grids.
2) Application and further detailing of the proposed framework in an offshore wind farm case study.

The rest of the paper is organized as follows: The framework is introduced in section II where its elements covering virtualized intelligent electronic devices, software-defined networking model and quality of service, as well as cyber security surface of attacks are detailed in subsections II-A, II-B, II-C respectively. Then, an offshore wind farm case study is analyzed in section III. Finally, the conclusions are resumed in section IV.

II. Framework for Virtualized Intelligent Electronic Devices in Smart Grids

The proposed simulation framework serves as an advanced testing and analysis tool for critical cyber-physical energy system developments. It comprises of a hardware/software vIED setup, networking, and cyber security components (see Figure 1). In the following subsections (II-A, II-B, II-C), the three main elements of this setup are further detailed.

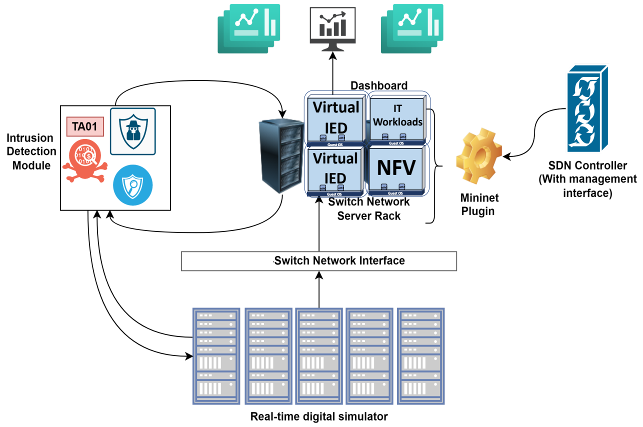
Dashboard
Intrusion Detection Module
TA01
Virtual IED
IT Workloads
Virtual IED
NFV
Switch Network Server Rack
Mininet Plugin
SDN Controller (With management interface)
Switch Network Interface
Real-time digital simulator

Fig. 1. Framework for Virtualized Intelligent Electronic Devices in Smart Grids including a real-time physical simulator, an SDN controller, and an intrusion detection module.

A. Virtual IEDs

IEDs represent a communicating device executing a functional application (e.g., over/under voltage protection, voltage regulator automation, wind farm controller, gateway, etc.) that stores and exchanges data with other IEDs through digital ethernet. The implementations of physical IEDs currently encounter several possible challenges including: (i) device failure; (ii) reconfiguration limitations; (iii) interoperability; (iv) costly deployment and upgrade efforts; and (v) external electrical disturbances, anomalies, and cyber threats [2], [3].

The concept of 'virtual' IEDs or vIEDs emerges as part of grid modernization efforts of the legacy hardware infrastructure. vIEDs follow a software-centric approach that decouples the functional domain logic from their physical implementations. The vIEDs instances are orchestrated by a real-time virtualization software that acts as the interface with the underlying standardized hardware server as seen in Figure 2. It can be noted that physical remote I/O, sensors, and hardwired actuators can never be virtualized, considering the definition of vIEDs.

Compared to physical IEDs, transitioning to vIEDs is motivated by different operational use cases with attractive benefits, including [3]:

1) Reducing deployment efforts of physical IEDs in terms of: (i) reduced number of hardware devices; (ii) lower deployment time (central/remote management); (iii) increased consistency and portability.
2) Testing environment equivalent to final deployment setup with support for legacy operating systems.
3) Backup to physical IEDs for inherent redundancy: (i) reduce system downtimes in case of provisioned ICT maintenance; (ii) automate disaster recovery mechanisms in case of ICT anomalies or cyber attacks.

On the practical side, vIEDs can co-exist with (or even replace) physical IEDs. Each vIED instance represents a virtual machine VM or container with functional logic and

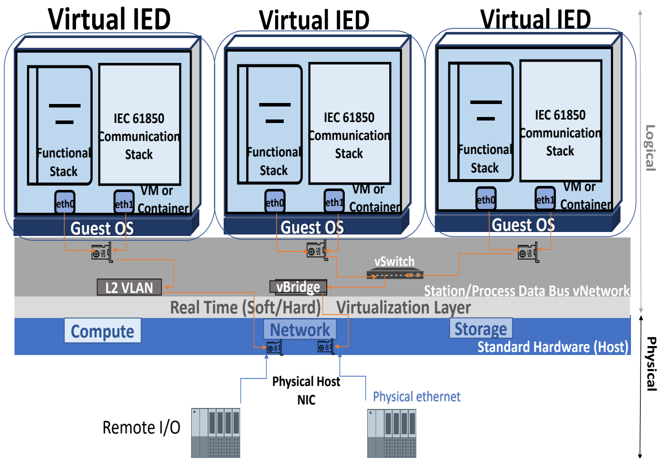

Fig. 2. The vIED concept running on a host machine with a configured internal network and based on an IEC 61850 communication stack maintaining interoperability based on [3].

a communication stack. A fundamental requirement for a software-centric approach of vIEDs is assuring interoperability between the deployed software. Hence, the IEC 61850 data model for power automation can be utilized to maintain interoperability between the communicating vIED instances [3].

The network between inter-vIEDs and external communications is logically configured at the level of the host server. Support for Layer 2 (MAC addressing) with routable internet protocol (IP) as well as standard IP networking (using virtual switches) is possible. The scheduling of the physical host resources is automatically done by the virtualization layer (e.g., hypervisor, container engine virtualization software).

Transitioning into virtual instances of networks and IEDs deployed alongside their physical counterparts requires advanced network management. Subsequently, adopting software-defined networking (SDN) to manage such networks is a possible solution. SDN provides a centralized approach for network configuration, management, and security, providing macroscopic visibility to the controller's loads [7]. The following subsection details the network model and the desired performances.

B. SDN/NFV Network Model and Quality of Service

Physical deployments of networking devices such as switches, routers, gateways, load balancers, and firewalls are usually used to monitor and manage local area networks (LANs) and wide area networks (WANs). With network function virtualization (NFV), these physical networking equipment are virtualized by deploying VMs that softwarize the network functions [8]. Several vIEDs and NFV VM instances can then be deployed on the underlying hardware following a multi-tenancy scheme. In this multi-tenancy scheme, the vIEDs and NFV instances 'share' the overall computational and storage resources while assuring run-time isolation.

Deploying vIEDs requires system operators to re-architect their substations and control rooms as micro data centers where racks of servers host the vIEDs and NFVs or container-based instances [9]. At the host server (LAN) level, an internal network with a virtual gateway is required for external and inter-communication within vIEDs, and NFVs.

Figure 3 illustrates a possible bridged network setup to allow the vIEDs to communicate with each other, with external physical IEDs, other tenant NFV implementations, and ultimately, to the control center applications via dynamic IP addressing and network address translation (NAT) capabilities. Several packets are routed through the network within the bandwidth, throughput, and channel constraints defined at the management plane (LAN or WAN) level.

Taking the case of digital substations, network packets include delay-sensitive or hard real-time stack (HRTS) messages and delay-tolerant or soft real-time stack (SRTS) messages such as IEEE 1588v2 or for time synchronization IEC 61850 L3 protocols [10]. The HRTS is in the order of a few ms and requires a robust and resilient underlying communication framework that maintains the intended quality of service (QoS) and recovers quickly from failure.

In the case of congested networks, QoS task and resource allocation techniques such as packet prioritization, traffic shaping and policing, and bandwidth calendaring are deployed to resolve the congestion and quickly restore the communication network to the desired performance levels.

For instance, QoS techniques allocate resources dynamically to prioritize the HRTS messages while ensuring that the SRTS messages stay in the buffer for a short time. Several traffic scheduling mechanisms can handle the pending packets or frames at the buffer. Additionally, each packet header for the HRTS and SRTS messages has a priority tag used by the networking devices to manage the inbound traffic. Physical network interface cards (NIC) that directly route the physical traffic to the vNIC attached to the vIED or NFV function are preferred as they provide faster performances than regular ethernet NICs with bridged networks (vSwitches) [11].

However, virtual setups coupled with physical communication infrastructure and software-defined networks encounter several performance concerns which can be monitored at the level of the SDN controller.

a) Resource Scheduling and Device Failures: vIEDs and NFV instances are susceptible to hypervisor/container engine failures. When the server is overwhelmed with tasks, it may switch to an inactive (blocked) mode. This interferes with the operation of the deployed vIED. Also, the maximum number of deployed instances that conserves the expected deterministic time responses [8] is constrained by the computational and storage capabilities of the host server. Additionally, the overall network is susceptible to physical device failures. From a design perspective, it is essential to have redundant systems in parallel with the main host/device pending recovery [7].

b) Network congestion and service loss: SDN controllers, in clusters, communicate with each other using East-bound and West-bound interfaces. The same redundancy is applied at both physical and logical (ether-channel) levels for the communication links. When one link is down, the traffic

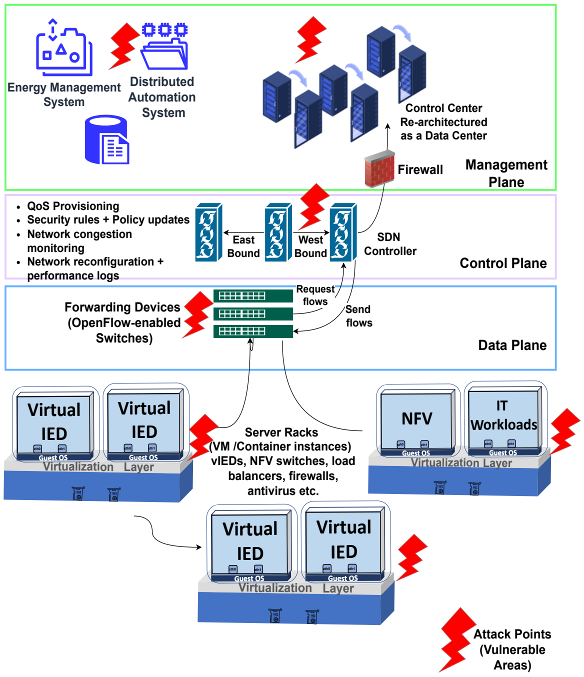
Energy Management System
Distributed Automation System
Control Center Re-architectured as a Data Center
Firewall
Management Plane
• QoS Provisioning
• Security rules + Policy updates
• Network congestion monitoring
• Network reconfiguration + performance logs
East Bound
West Bound
SDN Controller
Control Plane
Forwarding Devices (OpenFlow-enabled Switches)
Request flows
Send flows
Data Plane
Virtual IED
Virtual IED
Guest OS
Virtualization Layer
Server Racks (VM /Container instances) vIEDs, NFV switches, load balancers, firewalls, antivirus etc.
NFV
IT Workloads
Virtual IED
Virtual IED
Attack Points (Vulnerable Areas)

Fig. 3. Communication network model managed under the SDN framework and possible attack surfaces.

can be re-routed through a different link. To achieve such flexible re-routing: (i) a star, ring, or mesh network topology is adopted, and (ii) fault recovery policies and rules are defined in the SDN controller [12]. Networks often encounter an overflow of packets, mainly when a fault occurs in the power grid. A swift response is desired in such instances, and the communication framework should remain available. In collaboration with the load-balancing virtualization manager, the SDN controller clears the communication congestion through traffic policing techniques. The load balancer monitors the vIED workload and reassigns tasks appropriately [13].

Finally, for cyber security analysis in the proposed framework, the vulnerabilities and potential attack points in the system that intruders can compromise are identified. The next subsection defines the attack surfaces while discussing the consequent security challenges imposed on smart power systems.

C. Cyber Security of vIED/SDN Framework

An attack surface is a set of system resources and channels used by malicious actors to conduct cyber attacks on the system. Attackers exploit vulnerabilities and use various methods to breach the security of IT or OT systems and perform further averse cyber attacks. In the following, we analyze the attack surfaces introduced by the proposed framework, starting from the management plane to the server racks shown in Figure 3, and analyze the exploits. Such vulnerabilities are present in VM and container deployments, especially in the case of privileged host access [14].

1) Enterprise network: As illustrated in Figure 3, given that the management plane, i.e., control center, has an enterprise IT network with external connectivity, the vulnerabilities of the communication link to the outside network is the first possible attack surface. Within the control center, the energy management functions such as optimal dispatching, state estimation, and stability monitoring can be compromised. In [15], a risk analysis demonstrates the impact of such attacks on power system operation for a state estimator in the control center.

2) Man in the middle: A possible man-in-the-middle (MiTM) attack can occur on the communication channel to the SDN controllers, where an attacker can reach vIED and possibly download malware. Compromising vIEDs by malware may result in false control logic, measurements, protective commands, time stamp tampering, set point change, etc. Such events can directly disrupt power system operation, and stability [16]. For example, an attack scenario on the IEC 61850 communication standard, as described in [17], can be conducted on the vIED framework. In this case, the 'infected' protection vIED will send malicious tripping command to the circuit breaker forcing its opening.

3) SDN controller: SDN controller is another possible attack vector. If compromised or disrupted, the underlying data plane will be affected. In the proposed framework, the redundancy of the SDN controller makes it resilient against availability attacks. However, the SDN controller is also a possible critical target for planning the disruptive stages of the attack by monitoring the system network traffic. Thus, the cyber security of the SDN controller has the potential for further research.

4) Denial of Service: The denial of service (DoS) attack manipulates the network or computing resources' availability. In the proposed framework, SDN network switches and host operating systems possess limited processing power and memory. In a DoS attack, the attacker disrupts the running services and consumes the system's resources (e.g., consuming network bandwidth or overloading host memory with VMs).

5) Live Migration of vIEDs/NFVs: Migrating the states of a VM from one server to another without interrupting the running services is called live VM migration. Live VM migration is performed for several purposes, such as to avoid over-utilization of a physical server's resources, perform maintenance, and improve energy efficiency while providing seamless up-time and maintaining the best performance. Live VM migration is a good practice, especially for time-critical systems such as power systems. However, it poses a critical security threat. In [18], live VM migration attacks can cover both control and data planes for active and passive attacks. For instance, false data copying, data migration to the attacker's network, bandwidth manipulation, forced VM host migration, etc.

6) Multi-tenancy: Multi-tenancy is another possible security issue [19]. In multi-tenant servers hosting several vIEDs or NFVs, vIEDs share the same physical host. If a vIED is compromised via malware, the attacker might be able to access the shared memory of other vIEDs creating a VM information leak. Placing protection vIEDs along with less critical workloads poses an important security risk and a valuable target for attackers. Hence, it is a good practice to separate and isolate vIEDs by their function's criticality and implement the necessary communication rules via firewalls to prevent unauthorized access.

In the next subsection, we enumerate some solutions and countermeasures to address the issues imposed by the identified attack surfaces.

a) IEC 61850/62443: Given that the vIED relies on IEC 61850, this standard's previously known vulnerabilities (e.g., infected GOOSE traffic, authorizations) still apply [20]. One way to address this issue is to implement the IEC 62443 standard on top of IEC 61850 to improve cyber security [20]. However, this may not suffice the security requirements as the attackers learn new ways to intrude into the system. Smart intrusion detection systems (IDS) must be deployed as the second line of defense that actively monitors the IT/OT system and automatically detect cyber attacks.

b) IDS types and SDN/DoS: Mitigation of cyber attacks relies on accurate intrusion detection and prevention schemes. IDSs can be categorized into host-based and network-based depending on the target system they monitor. For malware detection in vIEDs, context-aware host-based IDSs can be used for system monitoring, e.g., system calls and executable binary codes. Network-based IDSs can detect attacks on the IT/OT communication network. Specifically, in the proposed framework, it is possible to implement a local detector at hypervisor level [21], which helps detect obfuscating malware. An IDS can also be placed at the control plane of SDN to obtain and inspect system-wide packets. The SDN controller can then be used to re-route the data flow through dynamic load balancing [22].

III. Offshore Wind Case Study

In the following subsections, we map the proposed conceptual multi-domain simulation framework to a concrete use case from the offshore wind domain. The idea is to validate the potentials mentioned above for a critical industrial application domain within different scenarios.

A. State-of-art of current offshore wind energy systems

The physical building blocks of traditional offshore wind farm systems managed by an operator include the wind turbines, offshore substations, and the onshore connection point to the Transmission System Operator (TSO). The subsystems go through very long physical installation, commissioning, and testing processes where compliance with grid codes is validated. On top of the physical layer, communication takes place with remote access thanks to the advanced SCADA systems monitoring the wind farm. Some of the benefits of Offshore Wind SCADA systems include:

- Remote visualization, diagnostic, and secure control of wind turbines and wind farm via transmission of real-time information and commands by standard industrial protocols
- Automatic regulation of turbines following grid code requirements
- Power measurements at the point of common coupling

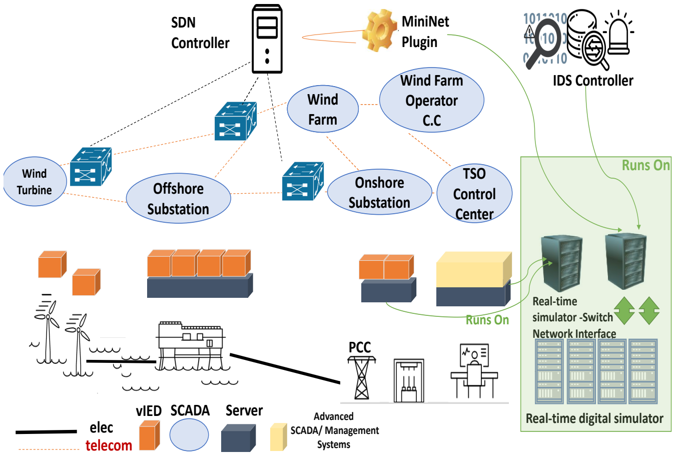

Fig. 4. The vision of future offshore wind energy systems and test simulation framework (green box).

The existing architecture is critical and requires high reliability and redundancy against physical grid failures as well as failures at the information and communication infrastructure level. However, operating and managing offshore farms' information and communication infrastructure requires significant efforts. Therefore, we propose a future vision for offshore wind farms SCADA system based on our setup and [9] to improve operational efficiency.

B. The vision of future offshore wind energy systems

The vision of future offshore wind energy systems mapped to the Virtualization/SDN/IDS schemes as seen in Figure 4 is the following:

- Proprietary physical IEDs are replaced with vIEDs running on top of standardized hardware.
- Offshore wind farms rely heavily on the data transferred between the wind farm and the remote control center to facilitate protection, automation, and control. A robust SDN-based communication framework with an IDS module ensures that the vIEDs, IEC 61850 servers (publishers), and data-in-transit are protected from malicious, unauthorized access while operating at the desired performance levels.

C. Simulation Framework

As seen in Figure 4, physical data is generated from a real-time digital simulator coupled with an industrial server running the vIEDs. IEC 61850 communication standard is mainly used for the local area (operational) networks LAN (at substation or wind farm levels).

The connection between the wind farm LAN and control center, otherwise through the wide area network WAN, is simulated by a software-defined networking emulator (here using MiniNET) linked to an SDN controller. Our proposed ecosystem includes an intrusion detection system for cyber attacks directly coupled with the network control plane and feedback from the host servers running the vIEDs. Therefore, both LAN and WAN cyber attacks scenarios can be researched.

The simplified model of a wind farm with an equivalent turbine, and protection and control of the offshore/onshore substation are simulated using the real-time (RT) grid simulator (physical plane). The infrastructure plane comprises of the external server coupled with the RT simulator running the different virtualized turbine, wind farm, and substation control and protection functions (data plane).

Finally, the supervisory or control plane monitors the network traffic to ensure performance, reliability, and security against external attackers using an IDS. Compared to current SCADA and security monitoring systems, the framework based on vIEDs, SDN, and IDS is semi-automated and orchestrated as opposed to error-prone and timely human interventions. The WAN can also be included in case a scenario including the TSO power grid model is required. We expect future offshore SCADA systems to co-exist with the advanced SDN and IDS systems.

IV. Conclusion

This paper presents the specifications of an innovative setup for testing virtualized IEDs coupled with smart grid networking and cyber security requirements. Technology constraints on the network performance and processing power are no longer the most prominent barriers against vIEDs. However, trust by power grid stakeholders such as TSOs and wind farm operators requires extensive testing of the maturity and reliability, especially for deterministic latency and networking bottlenecks. It was observed that migration of vIEDs due to device maintenance or external anomalies is interesting from an operational perspective yet poses significant security threats. Finally, the concepts have been mapped to an offshore wind SCADA case study with different scenarios.

Future works aim to add more precision to the wind farm case study and simulate a scenario with anomaly detection at the data model and the IT/OT protocol levels. Some of the aspects to cover are modeling the interaction between the wind farm operator's control center and the TSO control center since attacks on the wind farm may have system-wide effects. Also, considerations for case studies with deterministic latency involving time-sensitive networking and redundancy schemes need to be further developed.

References

[1] B. Hage Hassan, A. Narayan, M. Brand, and S. Lehnhoff, "Virtualization for performance guarantees of state estimation in cyber-physical energy systems," *Energy Informatics*, vol. 5, no. S1, p. 30, Sep. 2022.

[2] S. Ansari, F. Castro, D. Weller, D. Babazadeh, and S. Lehnhoff, "Towards Virtualization of Operational Technology to Enable Large-Scale System Testing," in *IEEE EUROCON 2019 -18th International Conference on Smart Technologies*. Novi Sad, Serbia: IEEE, Jul. 2019, pp. 1–5.

[3] N. Kabbara, M. O. Nait Belaid, M. Gibescu, L. R. Camargo, J. Cantenot, T. Coste, V. Audebert, and H. Morais, "Towards software-defined protection, automation, and control in power systems: Concepts, state of the art, and future challenges," *Energies*, vol. 15, no. 24, 2022.

[4] E. De Din, M. Pitz, F. Ponci, and A. Monti, "Implementation of the online distributed voltage control based on containers," in *2022 International Conference on Smart Energy Systems and Technologies (SEST)*. Eindhoven, Netherlands: IEEE, Sep. 2022, pp. 1–6.

[5] D. Rosch, S. Nicolai, and P. Bretschneider, "Container-based Virtualization of an IEC 61850 Substation Co-Simulation Approach," in *2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*. Milan, Italy: IEEE, May 2022, pp. 1–6.

[6] S. Attarha, C. Krüger, J. Kamsamrong, D. Babazadeh, and S. Lehnhoff, "A COMPREHENSIVE ANALYSIS OF THREATS AND COUNTERMEASURES IN VIRTUALIZED CYBER-PHYSICAL ENERGY SYSTEMS," in *CIRED 2021 - The 26th International Conference and Exhibition on Electricity Distribution*. , Online Conference: Institution of Engineering and Technology, 2021, pp. 1525–1529.

[7] C. Lee and S. Shin, "Fault tolerance for software-defined networking in smart grid," in *2018 IEEE International Conference on Big Data and Smart Computing (BigComp)*. IEEE, 2018, pp. 705–708.

[8] R. K. Barik, R. K. Lenka, K. R. Rao, and D. Ghose, "Performance analysis of virtual machines and containers in cloud computing," in *2016 international conference on computing, communication and automation (iccca)*. IEEE, 2016, pp. 1204–1210.

[9] P. Khajuria and D. Samara-Rubio, "Power of infrastructure modernization," *Intel Corporation*, 4 2021.

[10] S. Fang, Z. Li, and L. Huang, "New method to analyse delay of dds and mms in substation communication," *IET Communications*, vol. 14, no. 16, pp. 2794–2801, 2020.

[11] Y. Dong, X. Yang, J. Li, G. Liao, K. Tian, and H. Guan, "High performance network virtualization with sr-iov," *Journal of Parallel and Distributed Computing*, vol. 72, no. 11, pp. 1471–1480, 2012.

[12] A. H. M. Jakaria, M. A. Rahman, and A. Gokhale, "Resiliency-aware deployment of sdn in smart grid scada: A formal synthesis model," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1430–1444, 2021.

[13] Y. Su, P. Jiang, H. Chen, and X. Deng, "A qos-guaranteed and congestion-controlled sdn routing strategy for smart grid," *Applied Sciences*, vol. 12, no. 15, p. 7629, 2022.

[14] S. Sultan, I. Ahmad, and T. Dimitriou, "Container security: Issues, challenges, and the road ahead," *IEEE Access*, vol. 7, pp. 52 976–52 996, 2019.

[15] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3044–3056, 2019.

[16] S. Ansari, F. Castro, D. Weller, D. Babazadeh, and S. Lehnhoff, "Towards virtualization of operational technology to enable large-scale system testing," in *IEEE EUROCON 2019 -18th International Conference on Smart Technologies*, 2019, pp. 1–5.

[17] V. S. Rajkumar, M. Tealane, A. Ştefanov, A. Presekal, and P. Palensky, "Cyber attacks on power system automation and protection and impact analysis," in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, 2020, pp. 247–254.

[18] A. Choudhary, M. C. Govil, G. Singh, L. K. Awasthi, E. S. Pilli, and D. Kapil, "A critical survey of live virtual machine migration techniques," *Journal of Cloud Computing*, vol. 6, no. 1, p. 23, Dec. 2017.

[19] I. Odun-Ayo, S. Misra, O. Abayomi-Alli, and O. Ajayi, "Cloud multi-tenancy: Issues and developments," in *Companion Proceedings of The10th International Conference on Utility and Cloud Computing*, ser. UCC '17 Companion. New York, NY, USA: Association for Computing Machinery, 2017, p. 209–214.

[20] C. Jiwen and L. Shanmei, "Cyber security vulnerability assessment for smart substations," in *2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, 2016, pp. 1368–1373.

[21] S. Lata and D. Singh, "Intrusion detection system in cloud environment: Literature survey & future research directions," *International Journal of Information Management Data Insights*, vol. 2, no. 2, p. 100134, 2022.

[22] X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software-defined networking for smart grid resilience: Opportunities and challenges," in *Proceedings of the 1st ACM workshop on cyber-physical system security*, 2015, pp. 61–68.