A Real-Time Implementation and Testing of Virtualized Controllers for Software-Defined IEC 61850 Digital Substations

Kabbara, Nadine; Mwangi, Agrippina ; Ştefanov, Alexandru; Gibescu, Madeleine

DOI
10.1109/OJIA.2024.3426321

Publication date
2024

Document Version
Final published version

Published in
IEEE Open Journal of Industry Applications

Received 15 February 2024; revised 3 June 2024 and 25 June 2024; accepted 8 July 2024. Date of publication 10 July 2024; date of current version 24 July 2024. The review of this article was arranged by Associate Editor E. Stracqualursi.

Digital Object Identifier 10.1109/OJIA.2024.3426321

A Real-Time Implementation and Testing of Virtualized Controllers for Software-Defined IEC 61850 Digital Substations

NADINE KABBARA [1,2], AGRIPPINA MWANGI [2], ALEXANDRU ŞTEFANOV [3] (Member, IEEE), AND MADELEINE GIBESCU [2] (Member, IEEE)

[1]EDF R&D Paris Saclay, 91120 Palaiseau, France
[2]Utrecht University, 3508 TC Utrecht, Netherlands
[3]Delft Technical University, 2629 HS Delft, The Netherlands

CORRESPONDING AUTHOR: NADINE KABBARA (email: nadine.kabbara@edf.fr)

This work was supported in part by the European Union's Horizon 2020 Research and Innovation Programme under the InnoCyPES project (Innovative Tools for Cyber-Physical Energy Systems) and in part by the Marie Skłodowska-Curie under Grant 956433.

ABSTRACT This article implements and validates the performance of a virtual intelligent electronic device (vIED) framework for digital substations using a real-time (RT) simulation environment. The work looks toward the future design of protection, automation, and control systems, an evolution of the digital substation design based on IEC 61850 and virtualization technology. An RT simulation setup was developed to speed up and enhance the deployment and maintenance of vIEDs with a novel well-defined test methodology. Several scenarios were tested by varying the number of vIEDs and relevant (communication, scalability, and functionality) configuration criteria. In addition, we assessed the efficiency of a software-defined communication network for the vIED framework and its adaptability to dynamic scaling of the network under transient data traffic loads. The tests demonstrated the efficient performance of vIEDs across various system configurations, particularly for requirements on the response time and network transfer latency. The findings showcase the significance of proper design and testing methodology that can be benchmarked against other virtualization platforms for substation systems.

INDEX TERMS Cyber-physical power systems, digital substations, IEC 61850, software-defined network (SDN), virtual intelligent electronic devices (IED), virtualization.

I. INTRODUCTION

A cyber-physical power system consists of multiple subsystems, each with varying monitoring, management, and control levels [1]. The efficient operation of the power system involves real-time (RT) interpretation of extensive data from diverse sensing points, such as large-scale power plants, distributed energy resources, and remote merging units (MU) from high and medium-voltage substations. Transmission and distribution system operators manage several intricate information systems to ensure a reliable transfer of critical grid data inside and between substations as well as remote control centers (CC) [2].

A typical grid's information system involves numerous networking switches, routers, physical control devices, process control, relays, etc. A lot of these communicating devices are physically located at the level of digital substations. A digital substation represents a technological advancement over conventional substations by incorporating microprocessor-based intelligent electronic devices (IEDs), and advanced automation. Unlike traditional substations relying on analog technology and manual processes, digital substations use digital instrument transformers, and high-speed fiber-optic communication [3]. This shift enhances system accuracy, flexibility, and scalability, and enables RT monitoring, advanced control, and predictive maintenance use cases for the substation [3], [4].

The growing integration of distributed energy resources calls for more specialized controllers, leading to higher operational costs and complex development cycles [5]. The hardware infrastructure of traditional substation protection, automation, and control (PAC) systems can also be challenging to manage and maintain [6]. Upgrading the system to incorporate new advanced features is complex, and hardware failure events can be costly to repair [7]. There are also long-term uncertainties in system specifications and reliability concerns that can add to the challenges. Moreover, deployments and offline hardware in the loop simulations can be a manual and inconsistent process, which can lead to errors if not automatically validated [8], [9]. Therefore the legacy, yet functional technology can eventually restrict a faster innovation cycle in response to the evolving needs of modern power grids.

To overcome these challenges, there is a new trend in power system PAC design that involves separating functionalities from hardware-dependent implementations. As a result, more energy stakeholders are now interested in implementing adaptive systems, such as those offered by the information technology (IT) field with the reliability and security required for operational technology (OT) power assets [10]. This shift aims to transform traditional power grids into software-defined smart grids by embracing virtualization and software-defined technology. Motivated by the telecommunication industry's experience in modernizing their networking infrastructure with virtual network virtualization (NFV) [11], [12], the concept of virtual IED aims to provide the equivalent transformative model for future PAC hardware infrastructure.

Kabbara et al. [6], [13] describeD virtual IEDs (vIEDs) as a software-based implementation of IEDs in a virtual machine or container with functional logic (e.g., overvoltage protection, tap voltage regulator, or droop control algorithms) and an IEC 61850 communication stack. The virtual machine or container emulates the hardware resources (operating system, networking, etc) encapsulated within a software-defined environment [14]. Virtualization allows to optimize the host resources, enhance operation and management, with inherent backup recoveries [13]. The vIEDs concept aims to make use of the advantageous offered by virtualization technology to satisfy the power system's flexibility and operational needs. Similar to traditional physical IEDs, vIEDs interact with the process-level MU to exchange data and perform various functions within a digital substation. We hereby use the term virtualized controller (or relay) synonymously with vIED. The concept of vIEDs can be really useful for offline testing, operations and maintenance, and factory/site pre-acceptance simulation tests as a "digital twin" equivalent [15]. Also, vIEDs help in reducing the hardware footprint by replacing the numerous physical IEDs dispersed in a substation (CAPEX reductions). It thus offers compelling advantages in improving the system operation and maintenance needs [3]. However, time-sensitive data exchange between the vIEDs remains highly dependent on the efficiency of the underlying communication network.

Remodeling the substation communication network using software-defined network (SDN) was considered by [16], [17], and [18] as an essential step toward modernizing digital substations. SDN technology provides means to centrally monitor traffic for different communication network topologies. As such, the SDN-enabled network bus can allow dynamic network management for RT protection, automation, and control functions utilized by the vIED framework as demonstrated by [19]. These software-based implementations allow us to easily configure, deploy, and centrally manage the numerous virtual devices dedicated to substation automation systems [20].

However, integrating SDN and virtualization technologies into the digital substations requires a thorough assessment of their performance through advanced configuration and validation tests to guarantee that the solutions meet the desired performance requirements. This challenge motivates the need to propose novel simulation testbeds and design frameworks to foster vIED developments.

This article addresses a RT implementation and feasibility of IEC 61850 digital substation using virtual IEDs and SDN for the communications where the primary novelty is in the proposed formalized testing methodology and different advanced scenarios (covering functionality, scalability).

A. STATE OF THE ART

It is important to note that only literature that defines virtual IEDs, as indicated earlier in the Introduction, was considered. We deemed papers focusing on IED "cosimulation" without integrating virtualization as the implementation used in the test-bed as outside our area of focus. In this regard, previous studies have investigated different aspects of adopting a software-defined approach for digital substations using both SDN and virtualization technologies.

The concept of benchmarking the performance of vIEDs (particularly protection relays) was studied by quite a few authors in [21], [22], [23], [24], [25], and [26]. However, we noticed a difficulty in directly comparing the results of different studies due to the lack of a reference baseline for comparison. Also, no study yet tackles a hybrid setup with both virtual machines and containerized IEDs within a formalized test methodology.

Concerning SDN studies, the authors in [27] and [28] analyzed SDN architectures and their suitability for IEC 61850 digital substations in terms of performance and security. Similarly, Li et al. [29] proposed to improve the bandwidth of substation communication networks based on IEC 61850 using a modified SDN controller communicating with the IEDs. A dynamic bandwidth allocation policy is implemented and mapped to the abstract services provided by IEC 61850 to provide interoperability between the SDN controller and the IEDs. Results show that the bandwidth utilization can be improved up to 90%. However, the work by [29] did not utilize the actual IEC 61850 communication stack and only modeled and simulated the generic object-oriented substation event (GOOSE) protocol transmission delay. Also, no coupling to a RT digital simulator or vIEDs was implemented.

The authors in [30] developed an SDN setup for measuring IEC 61850 Quality of Service (QoS) using Mininet [31] and OpenDaylight Controller [32]. An overcurrent fault event with

GOOSE trip signals was benchmarked for different QoS policies with a stress condition on the connecting links. However, functional tests on the IEC 61850 data model and a detailed test setup were not studied in the papers mentioned above.

Concerning studies that combine both SDN and vIEDs, Leal and Botero [33] primarily proposed and detailed an architecture based on SDN for digital substations with IEC 61850. Leal and Botero [33] discussed the use of IED virtualization using unikernel as means to optimize system commissioning. However, the article did not tackle any implementation of the proposed concept within the SDN framework. To the best of our knowledge, Rösch et al. [19] first demonstrated the feasibility of a hybrid vIED/SDN setup but was limited to basic delay testing without advanced data model configurations or scale up tests with hybrid containers and concurrent SV streams.

B. PAPER CONTRIBUTIONS AND ORGANIZATION

As a summary, we noticed that studies in the field of vIEDs are still limited regarding both simulation setup configurations without a well-defined testing methodology. A hybrid setup with vIEDs, in both VMs and containers, coupled to a software-defined communication network is yet to be tested with a real industrial IEC 61850 substation configuration description (SCD) file. Also, most studies primarily focus on setup validation for basic performance, and no advanced configuration scenarios covering practical and functional aspects covering scalability have been tested.

The main contributions of the article are as follows.

1) *Design and test methodology* for a setup with virtualized IEDs running on a software-defined communication network and coupled to an RT digital simulator.
2) *Validate and benchmark the setup* for different configuration scenarios covering communication, functionality, and scalability aspects with a real industrial IEC 61850 SCD file using an IEEE 5-bus model.
3) *Support performance testing* of the software-defined communication network with hybrid vIEDs and dynamic data traffic with concurrent SV streams.

The rest of this article is organized as follows: Section II describes the software-defined vIED framework. Section III describes the evaluation setup and methodology. Section IV discusses the results of the benchmark tests for the deployed vIEDs and the efficiency of the software-defined communication network. Finally, Section V concludes this article.

II. BACKGROUND AND OVERVIEW

A. IEC 61850 OVERVIEW

The IEC 61850 standard is used for power system automation to facilitate communication between devices in electrical substations and related systems. It focuses on the exchange of information and control commands between various devices like protection relays, switches, meters, and more, which are involved in managing and safeguarding electrical grids. The standard also defines a common language that describes how data should be structured, organized, and transmitted in terms of data semantics and syntax (logical devices, nodes, objects, attributes). It thus helps ensuring that different manufacturers' equipment remains interoperable making it easier to build and maintain complex power systems [17].

The "substation configuration language" (SCL) is defined as part of the IEC 61850 standard. SCL is a standardized extensible markup language (XML) format that is used to describe the configuration and communication settings of devices within communication settings, data mapping, and logical nodes. In this work, a real SCD file describing the topology of a digital substation with MU and protection IEDs was utilized to configure the simulated vIEDs.

B. HYBRID IEC 61850 DIGITAL SUBSTATION ARCHITECTURE WITH VIRTUALIZATION

Fig. 1 illustrates the IEC 61850 digital substation architecture. At the bottom, the power systems equipment, such as current/voltage transformers (CT/VT), switchgear, and sensors are connected to the MU. The MU is connected to the instrument transformers through copper wire or is embedded in nonconventional instrument transformers. The standard defines two separate "bus networks" depending on their physical placement in the substation and the criticality of the communication traffic: process and station buses. The MU digitizes the analog measurements from the power system equipment and publishes them (as unicast or multicast ethernet frames) over the Ethernet-based process bus as sample value streams (as stipulated in the IEC 61869-9 Instrument transformers - Part 9: Digital interface for instrument transformers) [34]. Critical traffic, such as GOOSE, SV, or PTP normally flows in process bus networks while manufacturing message specification (MMS), NTP, FTP, etc., flow in station bus networks.

At the process level, the IEDs subscribe to the SV data. These IEDs analyze the SV stream payload and react to the data based on its configuration and functionality. In this framework, vIEDs are deployed at the bay level and they communicate with MUs and other IEDs to exchange GOOSE messages. In their design, the vIEDs, modeled as containers, use an IEC 61850 library [35] built on (SCL) that defines the data model and exchange. Using these IEC 61850 SCL files, system operators can configure and commission devices in a substation more efficiently. This saves time and reduces the complexity of setting up and maintaining a modern electrical substation. The left side of the figure showcases the IEC 61850 data model mapping of the simulated MU and IEDs as extracted from the SCD file. The main data signal (or logical nodes as per IEC 61850 terminology) include the trip (PTRC), alarm action at overthreshold (FXOT), time overcurrent protection (PTOC), and control (CSWI/XCBR).

At the station level, the IEDs send MMS data to the CC for storage and reporting. Notably, the protection and control team at the CC can send commands through the station bus to the IEDs, MUs, and circuit breakers as needed. On the communication side, Fig. 1 illustrates 1) the process bus that links the MUs to the IEDs and 2) the station bus that links

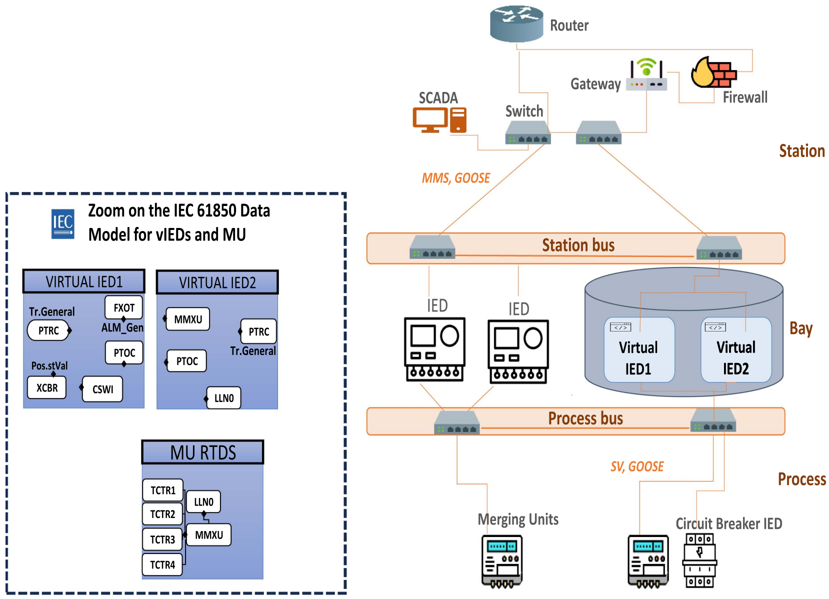


FIGURE 1. **IEC 61850 digital substation communication architecture adapted for the software-defined vIED framework (right) with a zoom on the associated data model mapping within each vIED and MU (left).**

the IEDs to the SCADA and the IT enterprise network. The CC/SCADA sends control commands to IEDs that are connected to the station bus on a dedicated network interface. In general, the CC/SCADA does not directly interface with process bus IEDs, with some exceptions as in the case where process and station buses are confounded. Due to implementation issues or budget limitations, some vendors of IEC 61850 digital substation architectures use the same physical network switches for both the process and station buses with VLAN to segregate the networks logically. IEDs at bay level can interface with the process bus, where the network access separation helps satisfy security and management requirements. The bay IED then sends a digital control signal to the appropriate MU and/or circuit breaker IED that actuates its opening/closing.

The critical, time-sensitive process bus must remain reliable hence we leverage the benefits of SDN in the design of the process bus [34]. On the other hand, the station bus is critical but less latency-sensitive and can run on the normal Ethernet infrastructure [36].

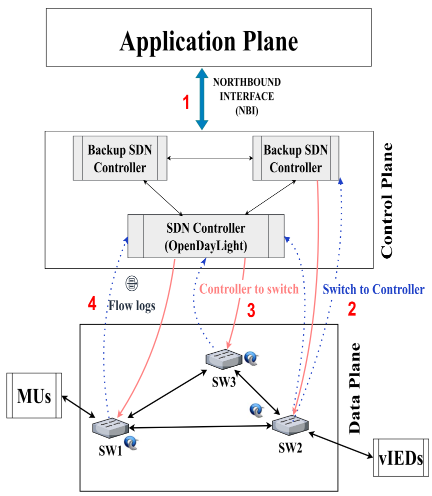


FIGURE 2. **SDN schematic comprising the application, control, and data plane used to facilitate interaction (numbered sequentially) between the Merging Unit (MU) and the vIEDs.**

C. SOFTWARE-DEFINED NETWORK ARCHITECTURE

Fig. 2 illustrates the software-defined architecture used to model the process-level communication network for the vIED framework. In principle, SDN decouples the control plane from the data plane providing a central point of management for the network under its administrative domain. The data plane interacts with the SDN controller using OpenFlow protocol at the southbound interface. Further, the SDN controller interacts with network management applications on the application plane at the northbound interface through the RESTCONF protocol. Two possible network management strategies can be deployed by the SDN controller: 1) reactive and 2) proactive. A reactive mode corresponds to a basic mode of operation that treats packets as soon as they arrive with no preconfigured or corrective strategies anticipating critical traffic patterns. A proactive mode can integrate preconfigured rules that anticipate network traffic events and allow to react before a critical network event occurs. A simple reactive mode was chosen for our SDN controller in this study.

When the MU digitizes the analog current and voltage measurements, it sends them as IEC61850 SV ethernet frames to the ingress port of SW1 (see Fig. 2). SW1 reads the ethernet frame and looks up its flow table for instructions on how to forward the frame. If no matching flow exists, it sends the frame to the SDN controller to request flow information to

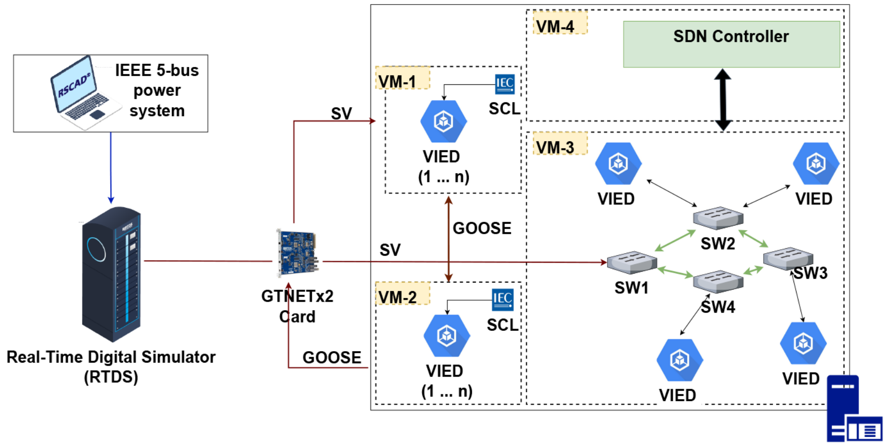


FIGURE 3. Hybrid software-defined vIED testbed (on process bus) coupled to a RT power system simulator (RTDS) where the MU publisher is within RTDS. vIEDs within VM-1 and VM-2 *directly* communicate with the RTDS GOOSE/SV GTNET card. vIEDs within VM-3 *indirectly* communicate with the GTNET card passing through the Mininet Network.

the desired destination node. The SDN controller sends flow instructions into the switch's flow table enabling the switch to forward the frame. In the design, the control plane is configured as a cluster to avoid having it as a single point of failure hence (1, .., n) controllers are configured with one being the primary controller and the others connected to it as backup controllers.

In this article, a software-defined process bus is validated to determine its ability to deal with sudden, unexpected network traffic spikes (for instance, when SV and GOOSE messages are suddenly transmitted during a failure causing a sudden increase in network traffic load) using traffic engineering methods, such as rerouting and load balancing configured in the SDN controller as features. Further, scaling digital substations with traditional network architectures not only leads to huge capital and operational expenses but also increases the network complexity [37]. Therefore, this work will evaluate the impact of scaling nodes on the robustness of the proposed SDN-enabled process bus with stress tests having forced packet drops.

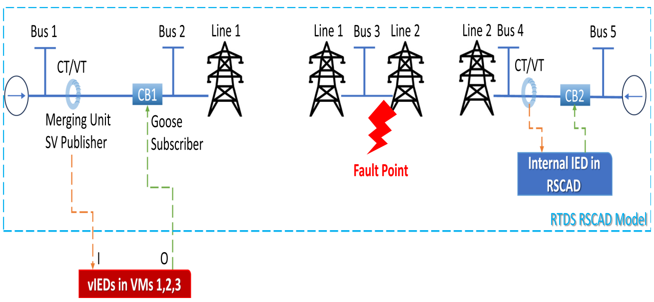


FIGURE 4. IEEE 5 bus power grid model coupled with internal (inside RTDS) and external virtualized IEDs (in containers).

TABLE 1. Physical Server and Virtual Machine Specifications

Physical server specifications	Intel Xeon CPU 3.60GHz, 64GB of RAM, PROXMOX hypervisor
Virtual Machine specifications	Intel 4 cores, 16GB RAM, 82GB Hard Disk Ubuntu 22.04 operating system

III. REAL-TIME SOFTWARE-DEFINED VIED SETUP

A. EVALUATION SETUP

A hybrid testbed, as illustrated in Fig. 3, was designed to conduct the validation tests for the vIED framework. The RTDS sampling rate was 50 ms. The simulation sampling interval for SV streams was 80 samples per cycle (4 kHz for 50 Hz and 4.8 kHz for 60 Hz nominal power system frequency, respectively). In the setup, a 60-Hz system was simulated. An IEEE 5-bus test system (see Fig. 4) was modeled on RSCAD software and simulated on the RT digital simulator (RTDS).

The RTDS's GTNETx2 card communicates the IEC 61850 SV, GOOSE, and MMS messages from the simulated IEEE 5-bus model to the physical server, with hardware specifications denoted in Table 1. This physical server contains four virtual machines as follows.

1) *VM-1 and VM-2:* The VMs run an overcurrent protection logic with an IEC 61850 GOOSE/SV publisher and subscriber. VM-1 is responsible for subscribing to the published SV and issuing a first alarm (ALM) signal to VM2 in case an overcurrent is detected as an MMS report or GOOSE message depending on the test scenario. VM-2 is responsible for verifying the alarm signal and issuing a final GOOSE tripping signal to actuate the circuit breaker of the controlled bus. The VM image is based on the open-source code available at [38]. Also, up to ten vIED docker containers based on the same image were deployed in parallel to the bare image in the VMs. The docker containers run on their internal bridged network linked to the VM's network which communicates with the RTDS GTNETx2 card.

2) *VM-3:* The Mininet [31] emulator was installed to model the SDN for the bus of the vIED framework. The vIEDs in VM-3 have been deployed as bare Mininet hosts.
3) *VM-4:* The OpenDayLight [32] SDN controller (ver-0.8.4) running on OpenFlow 1.3 protocol was installed. This is the control plane of the SDN architecture that remotely connects to VM-3 via an IP address.

It is important to note that in our setup, VM-1 and VM-2 are dedicated for vIED framework testing, while VM-3 and VM-4 are dedicated to the SDN communication performance. The internal IED in RSCAD is used as a backup that should automatically trip CB2 in case the vIEDs are too late to trip CB1 and clear the fault. All trip signals are sent via the GOOSE protocol. The vIEDs (in VM-1, and VM-2) do not directly communicate with the RSCAD IED but can communicate internally over the virtual bridge network over GOOSE messaging.

B. METHODOLOGY

1) FOR THE IEC 61850 VALIDATION TESTING OF VIED FRAMEWORK

The IEEE 5-bus power grid model (see Fig. 4) generates IEC 61850 SV, MMS, and GOOSE messages that are transmitted to both the internal IEDs (hosted inside RTDS/RSCAD) and external vIEDs (hosted on VM-1 and VM-2). The choice of an IEEE 5-bus model was sufficient for our investigations as we focused on simulating local interactions at the level of a single digital substation. The scalability of our framework concerns increasing the number of virtual IEDs and the information exchanged at the level of the communication network.

The chosen grid model has two controllable circuit breakers (CB1 and CB2). CB1 is controlled by the external virtualized IED simulated in the physical server connected to the local RTDS subnetwork. CB2 is controlled by the internal protection IED simulated inside the RTDS model. The internal IED was used to compare the expected behavior with the one from the vIED.

A merging unit that has been simulated inside the RTDS RSCAD environment is responsible for publishing the measured voltages and currents of a particular bus (as per IEC 61850 sampled values). In addition, the IEEE 5-bus model was configured with a GOOSE communication interface that can subscribe to external trip signals from the vIEDs.

The vIED IEC 61850 communication stack has been instantiated with a real substation commissioning project SCD file from EDF R&D. It was decided to map one vIED per VM, with the addition of multiple other containers within the same VM for scalability testing and mimicking extra resource usage. The choice of using two separate VMs instead of a single VM with more allocated resources is to test the limits of more data exchange between the internal vIEDs virtual network. Different protocol choices (here MMS reports and GOOSE control blocks) between the VMs were also tested.

2) FOR THE SOFTWARE-DEFINED COMMUNICATION NETWORK PERFORMANCE VALIDATION

A controlled test environment that mimics the actual process and bay-level bus for the vIED framework was designed on the Mininet emulator, as shown in Fig. 3. SV streams are polled to the Mininet virtual hosts from RTDS's GTNETx2 card using socket binding and then published to a multicast onto the Mininet network. For scaled-up test scenario, Mininet hosts were also used to publish more SV streams into the switch network. On the other end, vIEDs (modeled as Mininet virtual hosts) subscribe to the incoming SV streams. Host1 on switch 1 subscribes to the SV from RSCAD (using SOCKETs) and pushes a GOOSE that is subscribed by host3 on switch 3.

Different case scenarios were defined for MUs and vIEDs in scaled networks with varied traffic loads to perform comprehensive validation tests. In all these case scenarios, network data traffic was extracted using the iperf3[1] network throughput management tool and the Wireshark[2] network monitoring tool. The iperf3 tool is launched between a source node and a destination node. It runs in the background as different actions are taken on the network topology, such as dropping links, increasing network traffic, and shutting down switches. Then, the iperf3 collects the latency, bandwidth, and round trip time statistical data into a JSON file. The iperf3 plotter tool and iperf3 preprocessor tools are used to plot out the different case scenarios under different network traffic loads and scaled hosts. The SDN initial flow setup delay is monitored by analyzing the packets in Wireshark.

IV. RESULTS OF VALIDATION TESTS

A. VIEDS PERFORMANCE TESTING FOR REAL-TIME PROTECTION

The authors in [19], [21], [23], [24], and [25] analyzed the performance of various time-sensitive vIED frameworks by measuring the following.

1) The "transfer time" as per IEC 61850 (from the moment the fault is measured by the MU until the concerned IED receives the fault information).
2) The total response time (from the start of the fault until the signal trip is TRUE).
3) The total fault clearing time (from the start of the fault until a CB is OPENED with a cleared fault).
4) The cyclic execution time (part of the vIED processing time and concerns the execution rate of the behavioral logic).

The total end-to-end time delays from the start of a fault can be seen in Fig. 5. We note that the serial cable and MU processing delays are neglected in this study. The transfer time currently has an absolute reference that shall not be passed (less than 3 ms), as specified in the IEC 61850 standard [40].

[1][Online]. Available: https://github.com/ekfoury/iperf3_plotteriperf3 network throughput management tool

[2][Online]. Available: https://www.wireshark.org/Wireshark network monitoring tool

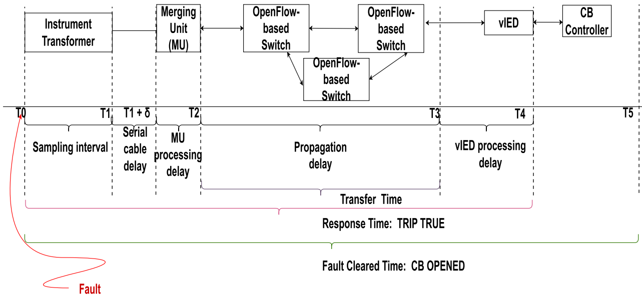


FIGURE 5. End-to-end time mapping of a software-defined process bus linking the MU to the bay-level vIEDs [39].

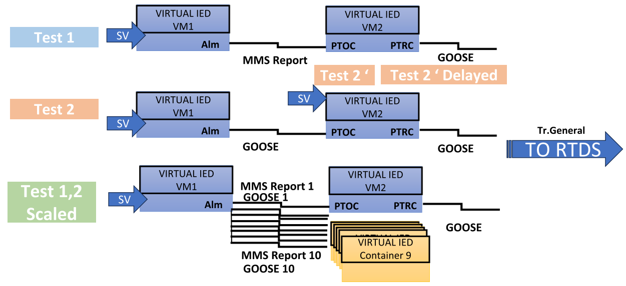


FIGURE 6. Six different test cases of the vIED setup with modifications of the IEC 61850 exchanged data protocols, number of vIEDs, and vIED functional changes.

The total response and fault clearing times reference values depend on other functional (algorithmic) factors. For instance, the overcurrent protection algorithm can have different time delays as a function of the fault current magnitude. Subsequently, a faster response time of a vIED compared to a physical one can be purely based on a functional change. The maximum allowed fault clearance time in the transmission network is typically less than 100 ms, being 2–3 cycles typical values for the primary protection systems. Higher fault clearance times are normally adopted in distribution networks [13].

In this article, we focus on measuring the average total response and fault-clearing times to perform a preliminary validation of the developed setup. The transfer time was first not explicitly measured but was just observed. An assumption was made to consider the time dependence delay in the overcurrent protection algorithm to be close to zero for the baseline test cases. Other time measurements (cyclic execution time, jitter) can be conducted in case the setup is optimized for RT deterministic evaluation.

Testing how fast the framework adjusts to different network setups, load changes, or system reconfigurations is crucial. It shows how agile the framework is in handling dynamic situations while keeping up its performance. Three main configuration criteria were classified for assessing the performance of the vIEDs as follows.

1) *C1 Communication Protocol and Exchanged Data:* Different IEC 61850 data models were tested with a focus on changing the protocol used for data exchange of the trip signal (through an SCD file modification for reports and GOOSE control blocks).
2) *C2 Scalability:* A focus on the number of vIEDs concurrently running including hybrid containers and VMs.
3) *C3 Functional Changes:* A time delay in the overcurrent protection algorithm was included.

Six different test scenarios have been prepared for the vIED framework validation. The base scenarios consist of controlling a circuit breaker using a basic overcurrent protection algorithm (without a time delay) after a fault is triggered on the IEEE 5-bus grid model (see Fig. 6). In each test case, C1, C2, and/or C3 were modified. The test cases are explained in Fig. 6 and as follows in more detail.

1) *Test 1:* VM1 subscribes to SV packets from RTDS and issues an ALARM ON signal as an MMS report in case of a fault; VM2 is a client to the report and sends a TRIP TRUE as a GOOSE message.
2) *Test 1 Scaled:* Same as Test 1 with ten containers launched in VM2
3) *Test 2:* VM1 subscribes to SV packets from RTDS and issues an ALARM ON signal as a GOOSE message in case of a fault; VM2 is a subscriber of the GOOSE message and sends a TRIP TRUE.
4) *Test 2 Scaled:* Same as Test 2 with ten containers launched in VM2.
5) *Test 2':* VM1 is removed (to simulate a maintenance/upgrade situation); only VM2 is simulated as an SV subscriber that sends a GOOSE message TRIP TRUE after a fault.
6) *Test 2' Delayed:* Same as Test 2' with delay of 10 ms added to the overcurrent protection algorithm accounting for time delay as a function of the fault's current magnitude.

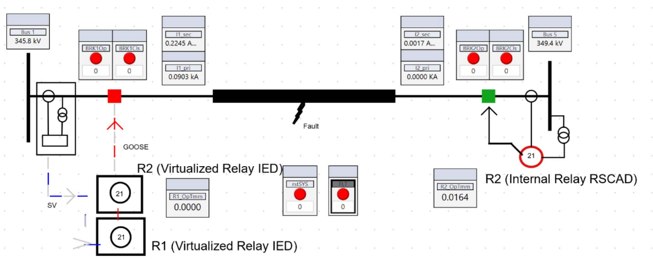
The benchmark consists of the results in Table 2 as a whole, which were extracted from the test scenarios and the RTDS results. Each test was repeated 25 times with the same VM and setup configurations, where a single-phase fault (on phase A of a line in the IEEE 5-bus system) was created in each test. The results with the TRIP signal status and the voltages and currents of phase A were registered and used for the benchmark. An example of the gathered data from the RSCAD environment can be seen in Fig. 7. The average fault clearing and response times from both internal (RTDS) and external vIEDs were measured focusing primarily on the latter. Some basic statistics on the measured samples, including standard deviation, minimum, and maximum values are also reported in Table 2.

In general, the results were coherent with the expected behaviors of the different configurations. More specifically, Test 1 and Test 1 Scaled had the longest average fault clearing and response time since the MMS report has a longer protocol transfer time. Test 1 Scaled had only a minor increase of less than 1 ms in trip time compared to Test 1. As for Test 2, the impacts of changing the protocol stack and a scaled environment with ten containers were tested. In general, the trip times for the internal protection from RTDS were fixed around 15 ms

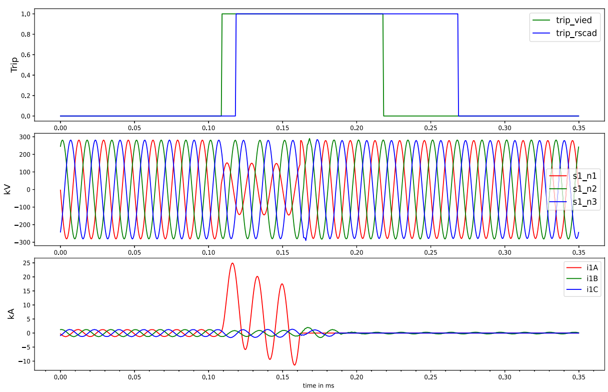
TABLE 2. Benchmark of the Evaluation Setup for the Different Tests 1, 1 Scaled, 2, 2 Scaled, 2', 2' Delayed Varying the IEC 61850 Data Model, Scalability and Functionality

Scenario	Fault Cleared	Response Time vIED:	Stdev	Min	Max
Test 1	104	52.1	0.4	51.3	52.5
Test 1 Scaled	150.6	53.3	0.76	52.3	55
Test 2	56.5	2.1	0.4	1.45	2.9
Test 2 Scaled	57.8	2.2	1.6	1.3	9.6
Test 2'	55.7	1.4	0.3	1.1	2.5
Test 2' Delayed	65.1	11.6	0.6	11.1	12.3

All response times are the averages of 25 tests and measured in ms.



(a)



(b)

FIGURE 7. Example of the monitored voltages and currents (V,I) read as SV from RTDS and treated by the vIEDs in the IEEE 5-bus test system with a fault simulated (a) and a Trip signal TRIP is sent from the internal RTDS logic (blue) and external vIEDs R2 (green) (b).

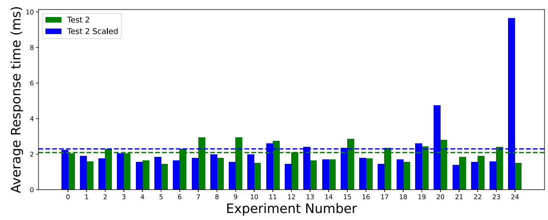


FIGURE 8. Benchmark Scaled versus Unscaled Test 2 with IEC 61850 GOOSE control blocks with 25 repeated experiments with average response time in (ms).

with negligible standard deviation. The fault clearing time measures the time between the fault is first detected until the fault is cleared and all currents are at zero due to the opening of CB1 or CB2 (trip from vIED or RSCAD).

As expected, the fault and trip times in Test 2 have considerably lower duration compared to Test 1 due to the use of the GOOSE protocol instead of the MMS report. We note here that the very low trip time compared to the internal RTDS relay trip is due to the lack of a time delay (varying as a function of fault current magnitude) within the overcurrent algorithm in VM2. The standard deviation of the 25 samples was less than 2 ms, showing a relatively stable reaction time despite the lack of optimized RT settings for the VMs, the host machine, and the bridged virtual network. However, since the setup is not optimized for RT conditions, in the case of the scaled Test 2, an outlier with a maximum of 9.6 ms was observed, which could be avoided with correct RT tuning. A more detailed comparison of scaled and unscaled responses with GOOSE messages can be found in Fig. 8. The figure shows a relatively stable average response time in the orders of less than 3 ms thus respecting the IEC61850 transfer time requirements.

For Test 2', the idea was to test a scenario where the vIED in VM1 was deactivated for an upgrade or some software maintenance. The data model in VM2 was modified to directly subscribe to the SV streams. The trip and fault clearing times with VM2, as the primary vIED, showed almost no differences compared to the divided case with two separate VMs. It was even faster by almost 0.6 ms on average. The 0.6-ms improvement is due to the lack of an extra GOOSE message that has to be treated and issued by VM1 before the final trip is sent. This shows that the modularity of the vIED image should be taken into consideration when designing the vIED topology. Also, the data model division into a single VM (here VM2) instead of two separate VMs can be more practical if sufficient resources are allocated to the VM (as detailed in Table 1).

As for Test 2' Delayed, the focus was on changing the functionality of the protection algorithm by adding a time delay following the detection of a fault. With a forced delay of 10 ms, the average trip time was at 11.62 ms, and thus, within the allowable margins. A standard deviation of 0.61 ms was recorded from the delayed tests. Thus, we confirm that no

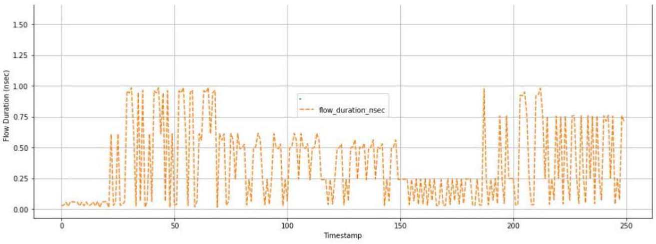
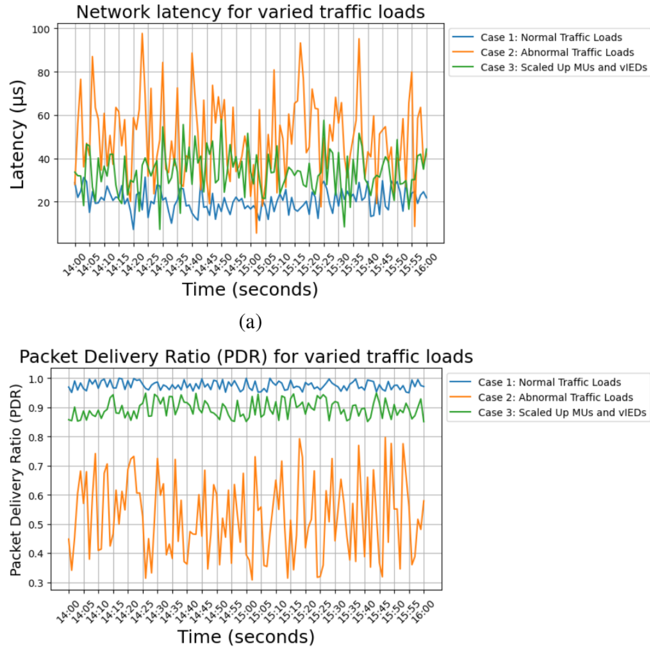


FIGURE 9. **SDN controller to Switch initial flow setup time where flow duration is the expiration time for the flow rule.**



(a)

(b)

FIGURE 10. **Proposed system model transient behavior measured using Iperf3 network throughput monitoring tool. (a) Network latency comparison across varying network traffic loads. (b) Packet delivery ratio for varied network traffic loads.**

particular impact on the performance is observed in case of a functionality change of the vIED.

B. PERFORMANCE TESTING FOR THE SOFTWARE-DEFINED COMMUNICATION NETWORK

We conducted performance tests for the software-defined process bus that connects the MUs to the vIEDs, as illustrated in Fig. 2. Several performance tests were conducted for the following scenarios.

1) *Case 1:* MUs running on the same local area network with the physical server (hosting vIED containers) with normal traffic loads.
2) *Case 2:* MUs running on the same local area network with the physical server (hosting vIED containers) with forced abnormal traffic loads and packet drops.
3) *Case 3:* Scaling MUs connected to a remote physical server (hosting vIED containers) while sending normal traffic loads.

The SV frames are received at the ingress ports of the SW1, as illustrated in Fig. 3. SW1 looks for flow instructions on how to publish the SVs onto the network from its flow table. If a flow is available, it publishes the SVs to a multicast address else, it sends a request for flow instruction to the SDN controller. The SDN controller, having a global view of the entire network, quickly ($\leq$ 100˜ns) sends a flow instruction for the shortest path to the destination, as illustrated in Fig. 9. On the other end, the vIEDs on SW2 and SW4 subscribe to the SVs.

Digital substation communication is latency-sensitive hence Fig. 5 was mapped out to denote the possible delay components for the bidirectional data exchange. All the delay components except the propagation (or transfer) delay, $\Delta t = (T_3 - T_2)$, are dependent on the vendor design specifications of the equipment.

Fig. 10(a) demonstrates the latency in the different case scenarios. We observed the transfer delay, Δt when sending SV and GOOSE messages through the Mininet switch network for the highlighted case scenarios in Fig. 10(a). In the 2-h long experiment, it was observed that the transfer delay between host 1 and 3 was in the range of $\geq 5\mu$s and $\leq 30\mu$s under normal traffic loads in case 1. An abnormal forced increase in network traffic was analyzed in case 2, especially during a fault scenario in the substation, which registered an increased latency and forced packet loss as the network was congested for stress case analyses. The latency was observed to have higher spikes and more volatility peaking at 100 ms for the passed packets.

Notably, case 3 showed scaling up the number of hosts to 15 MUs (adding an SV publisher stream from Mininet hosts in parallel with the RSCAD MUs) and 15 vIEDs. It was observed that under normal traffic loads from these devices, the switch network had an overall transfer delay, $\leq 60\mu$s with around 10% packet drops, as illustrated in Fig. 10(b). We infer that the 10% packet drops is primarily related to increasing the number of parallel SV streams as the explicit scalability Test1 and Test2 in results Section IV-A with only subscribing vIEDs did not show any noticeable packet drops. Abnormal traffic loads caused by sudden spikes in network traffic require proactive policies for load balancing and re-routing to maintain the overall latency within acceptable levels.

C. DISCUSSION

The benchmark testing showed a consistent response time, with average GOOSE trips under the 3-ms IEC 61850 transfer time requirement, as observed from the vIED and SDN normal network tests. However, laying more effort into the design of robust traffic engineering schemes (that would run as features in the SDN controller or as RESTFUL-based applications in the application plane) would help guarantee robust data exchange of the digital substation for scaled and abnormal traffic policies.

The point here was not to be fully and realistically representative of real networks. It was rather an example of how the testbed environment can support a more scaled network and some estimate of performance with the vIEDs running in parallel. Link parameters were adjusted to simulate real-life conditions, including link losses and bandwidth. An extension of the study may focus on reviewing the impact of proactive and autonomic efforts for traffic management (potentially considering cyber threats) and ensuring the scalability of networks, as proposed in [41].

As observed from the benchmark evaluations, it is necessary to have an absolute reference virtual IED from which different architectures and implementations can be compared. These reference metrics can include information that specifically appears for a virtualized implementation. For example, in addition to the expected transfer time, reference metrics on maximum allowed jitter (i.e., determinism) for a defined cyclic execution, and maximum memory consumption are possible examples.

Also, given that VM-4 has a dual role in simulating the SDN network and vIEDs, the effect of this dual role on the trip delay performance should be further analyzed. A larger testbed with more than one server with potentially some real switches with OpenFlow controllability can be used for more realistic SDN trip delay test scenarios.

V. CONCLUSION

This work conducted extensive validation tests for an RT virtual IED framework based on the IEC 61850 standard. An IEEE 5-bus power system model was simulated on RTDS to conduct RT protection with both internal RSCAD IED and external, docker-based vIEDs containers communicating within an SDN. Different test scenarios have been configured for validating vIED performance including various communication, scalability, and functional configurations.

The various system reconfigurations showcased the agility of the framework and its consistent performance regarding the vIED response time and network transfer latency. The test scenario when vIED in VM1 is deactivated for software maintenance and migrated to a mode with a single VM2 demonstrated that the modularity and exchangeability of the vIED image should be taken into consideration when designing the vIED substation topology. Using the SDN architecture in this setup demonstrated its feasibility for stress testing the network of virtualized digital substations across various traffic loads with some limitations in scalable and abnormal traffic scenarios. The observations showed that a well-defined design and testing methodology for virtualized substation systems is critical for supporting their rapid rollouts and benchmarking against other virtualization platforms.

The validation tests performed are comprehensive, yet further exploration through simultaneous fault occurrences would strengthen the assessment of the framework's robustness. Future studies can advance this work by adding vulnerability tests for common cyber-security threats in the validation process. Other types of tests not covered here include performance breakdown with parallel SV streams, optimization of resource allocation to the vIEDs, realistic network topology benchmarks, deterministic RT optimizations, different protocols for intra vIED to vIED communications, etc. Finally, exploring scenarios of communication failures during the framework's testing could provide valuable insights into its resilience and performance under adverse conditions especially scalability. The Containernet (a Mininet fork) [42] that works seamlessly with Docker containers could also be used to optimize the SDN host configuration and setup in containers.

ACKNOWLEDGMENT

The authors would like to thank the TU Delft IEPG Control Room of the Future (CROF) team for their invaluable contribution in setting up the testbed (Spring 2023).

REFERENCES

[1] A. M. Annaswamy, *Institute of Electrical and Electronics Engineers, and IEEE Standards Association, IEEE Vision for Smart Grid Controls: 2030 and Beyond*. New York, NY, USA: Instit. Electr. Electron. Engineers, 2013.

[2] "Advancements in centralized protection and control within a substation," *IEEE Trans. Power Del.*, vol. 31, pp. 1945–1952, Aug. 2016.

[3] Cigre Study Committee B5.60, "Protection, automation and control architectures with functionality independent of hardware," Cigre, Paris, France, 2022. [Online]. Available: https://www.e-cigre.org/publications/detail/891-protection-automation-and-control-architectures-with-functionality-independent-of-hardware.html

[4] G. R. Santos, E. Zancul, G. Manassero, and M. Spinola, "From conventional to smart substations: A classification model," *Electric Power Syst. Res.*, vol. 226, 2024, Art. no. 109887.

[5] H. Goyel and K. S. Swarup, "Cyber-physical system enabled smart grid based optimal controller placement," in *Proc. 21st Nat. Power Syst. Conf.*, 2020, pp. 1–6.

[6] N. Kabbara, A. Mwangi, M. Gibescu, A. Abedi, A. Stefanov, and P. Palensky, "Specifications of a simulation framework for virtualized intelligent electronic devices in smart grids covering networking and security requirements," in *Proc. IEEE Belgrade PowerTech*, 2023, pp. 1–6.

[7] M. Armendáriz, K. Paridari, E. Wallin, and L. Nordström, "Comparative study of optimal controller placement considering uncertainty in PV growth and distribution grid expansion," *Electric Power Syst. Res.*, vol. 155, pp. 48–57, Feb. 2018.

[8] B. Lundqvist and Y. Aabo, "The cost benefit of modern substation automation in electrical high voltage installations, ABB automation," 2002.

[9] J. Resch et al., "Engineering and validation support framework for power system automation and control applications," *e+i Elektrotechnik und Informationstechnik*, vol. 137, no. 8, pp. 470–475, 2020.

[10] C. Perducat, D. C. Mazur, W. Mukai, S. N. Sandler, M. J. Anthony, and J. A. Mills, "Evolution and trends of cloud on industrial OT networks," *IEEE Open J. Ind. Appl.*, vol. 4, pp. 291–303, 2023.

[11] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *IEEE Commun. Surv. Tut.*, vol. 18, no. 1, pp. 236–262, Firstquarter 2016.

[12] J. Matias, J. Garay, N. Toledo, J. Unzilla, and E. Jacob, "Toward an SDN-enabled NFV architecture," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 187–193, Apr. 2015.

[13] N. Kabbara et al., "Towards software-defined protection, automation, and control in power systems: Concepts, state of the art, and future challenges," *Energies*, vol. 15, no. 24, 2022, Art. no. 9362.

[14] A. K. Yadav, M. Garg, and Ritika, "Docker containers versus virtual machine-based virtualization," in *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2018*, vol. 3, Berlin, Germany: Springer, 2019, pp. 141–150.

[15] S. Ansari, F. Castro, D. Weller, D. Babazadeh, and S. Lehnhoff, "Towards virtualization of operational technology to enable large-scale system testing," in *Proc. IEEE EUROCON 18th Int. Conf. Smart Technol.*, 2019, pp. 1–5.

[16] Q. Yang and R. Smith, "Improve protection communications network reliability through software-defined process bus," in *Proc. Power Energy Automat. Conf.*, 2019, Art. no. 4.

[17] S. Meier, T. Werner, and C. Popescu-Cirstucescu, "Performance considerations in digital substations," in *Proc. 13th Int. Conf. Develop. Power Syst. Protection*, 2016, pp. 1–9.

[18] S. Gutierrez et al., "Next-generation power substation communication networks: IEC 61850 meets programmable networks," *IEEE Power Energy Mag.*, vol. 21, no. 5, pp. 58–67, Sep./Oct. 2023.

[19] D. Rösch, S. Nicolai, and P. Bretschneider, "Combined simulation and virtualization approach for interconnected substation automation," in *Proc. IEEE 6th Int. Conf. Smart Sustain. Technol.*, 2021, pp. 1–6.

[20] P. Vizarreta et al., "Incentives for a softwarization of wind park communication networks," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 138–144, May 2019.

[21] S. Schönborn, R. Birke, D. Kozhaya, and T. Sivanthi, "Real-time performance of virtualised protection and control software," in *Proc. 27th Int. Conf. Electricity Distrib.*, 2023, pp. 1817–1821.

[22] H. Falk, "Unified grid control platform," *Outside Box Consulting Serv., Smart Grid Forum*, 2022.

[23] R. D. F. Ferreira and R. S. de Oliveira, "Cloud IEC 61850 a case study of a software defined protection, automation & control system," in *Proc. IEEE 23rd Int. Conf. Emerg. Technol. Factory Automat.*, 2018, pp. 75–82.

[24] R. Wojtowicz, R. Kowalik, D. D. Rasolomampionona, and K. Kurek, "Virtualization of protection systems part 2: Tests performed on a large environment based on data center solutions," *IEEE Trans. Power Del.*, vol. 37, no. 4, pp. 3401–3411, Aug. 2021.

[25] D. Samara-Rubio, G. McKenzie, and P. Khajuria, "Virtual Protection Relay: A paradigm shift in power system protection," Kalkitech, Campbell, CA, USA, 2022. [Online]. Available: https://vpacalliance.com/data/files/virtualprotectionrelaywp-v051222-3.pdf

[26] M. T. V. Martinez et al., "Description of an edge computing solution to be used in digital substations," in *Proc. IEEE PES Innov. Smart Grid Technol. Eur.*, 2023, pp. 1–6.

[27] A. Kalra et al., "Using software-defined networking to build modern, secure IEC 61850-based substation automation systems," in *Proc. 15th Int. Conf. Develop. Power Syst. Protection Liverpool*, 2020, pp. 1–6.

[28] M. Girdhar, J. Hong, W. Su, A. Herath, and C.-C. Liu, "SDN-Based dynamic cybersecurity framework of IEC-61850 communications in smart grid," 2024, *arXiv:2311.12205*.

[29] G. Li, J. Wu, L. Guo, J. Li, and H. Wang, "SDN based dynamic and autonomous bandwidth allocation as ACSI services of IEC61850 communications in smart grid," in *Proc. IEEE Smart Energy Grid Eng.*, 2016, pp. 342–346.

[30] A. Leal, J. F. Botero, and E. Jacob, "QOS proposal for IEC 61850 traffic under an SDN environment," in *Proc. IEEE 10th Latin-Amer. Conf. Commun.*, 2018, pp. 1–6.

[31] "Mininet an instant virtual network on your laptop (or other PC)," [Online]. Available: http://mininet.org/

[32] T. L. Foundation, "Opendaylight (ODL)," [Online]. Available: https://www.opendaylight.org/

[33] A. Leal and J. F. Botero, "An architecture for power substations communication networks based on SDN and virtualization paradigms," *Revista Facultad de Ingeniería Universidad de Antioquia*, vol. 100, pp. 48–66, Jul./Sep. 2021.

[34] J. M. Mathew, D. Dolezilek, M. Katuru, and R. Karmaker, "Lessons learned from commissioning of IEC61850-9-2 process bus-based busbar protection system," in *Proc. 16th Int. Conf. Develop. Power Syst. Protection*, 2022, pp. 110–115.

[35] "libiec61850," [Online]. Available:https://github.com/mz-automation/libiec61850

[36] T.-Y. Wong, W.-H. Lau, H. S.-H. Chung, and C. Shum, "A feasibility study of using manufacturing message specification report gateway model for iec61850 inter-substation type-1 messaging over wide area network," *Sustain. Energy, Grids Netw.*, vol. 30, 2022, Art. no. 100612.

[37] A. A. Z. Soares et al., "SDN-based teleprotection and control power systems: A study of available controllers and their suitability," *Int. J. Netw. Manage.*, vol. 31, no. 3, 2021, Art. no. e2112.

[38] R. Massink, "IEC 61850 open server public," [Online]. Available: https://github.com/robidev/iec61850_open_server

[39] M. A. Aftab, S. S. Hussain, I. Ali, and T. S. Ustun, "IEC 61850 based substation automation system: A survey," *Int. J. Elect. Power Energy Syst.*, vol. 120, 2020, Art. no. 106008.

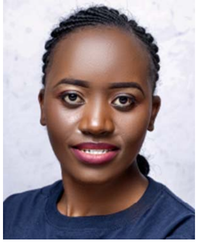
[40] *Communication Networks and Systems for Power Utility Automation - Part 5: Communication Requirements for Functions and Device Models*, Int. Electrotechnical Commission Standard, IEC 61850-5, 2013.

[41] A. Leal and J. F. Botero, "Defining a reliable network topology in software-defined power substations," *IEEE Access*, vol. 7, pp. 14323–14339, 2019.

[42] M. Peuster, H. Karl, and S. van Rossem, "Medicine: Rapid prototyping of production-ready network services in multi-pop environments," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw.*, 2016, pp. 148–153.

NADINE KABBARA received the M.Sc. degree in control and electrical engineering from Paris Saclay University, Gif-sur-Yvette, France, in 2021.

She is a third-year Industrial Ph.D. working with the French utility EDF in their R&D department. She is also part of the InnoCyPES European project on connected digital smart grids. Her research interests include digital substations, IEC 61850, virtualized IEDs, data modeling, and simulation frameworks.



AGRIPPINA MWANGI received the B.Sc. degree in electrical and electronic engineering from the Dedan Kimathi University of Technology, Nyeri, Kenya, in 2016, and the M.Sc. degree in electrical and computer engineering from Carnegie Mellon University, Pittsburgh, PA, USA, in 2021. She is currently working toward the Ph.D. degree in SDN IoT-edge networks for offshore wind farms with the Energy & Resources Group, Copernicus Institute of Sustainable Development, Utrecht University, Utrecht, The Netherlands.

Her research interests include IoT Edge, SDN, NFV, zero-touch networks, and smart grids.

ALEXANDRU ŞTEFANOV (Member, IEEE) received the M.Sc. degree in electrical power systems from the University Politehnica of Bucharest, Bucharest, Romania, in 2011, and the Ph.D. degree in cyber physical system modelling and coordinated restorations of power systems from the University College Dublin, Dublin, Ireland, in 2015.

He is currently an Assistant Professor of Intelligent Electrical Power Grids with TU Delft, Delft, The Netherlands, where he is also the Director of the Control Room with the Future Technology Centre. He is leads the Cyber Resilient Power Grids research group. His research interests include the cyber security of power grids, the resilience of cyber-physical systems, and next-generation grid operation.

MADELEINE GIBESCU (Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Washington, Seattle, WA, USA. in 2003.

She is currently a Full Professor of Integration of Intermittent Renewable Energy with the Copernicus Institute of Sustainable Development, Faculty of Geosciences, Utrecht University, Utrecht, The Netherlands. Since 2004, she has been working in The Netherlands in various academic capacities with TU Delft, Delft, The Netherlands; TU Eindhoven, Eindhoven, The Netherlands; and Utrecht University, leading research in smart grids and system integration of wind energy and solar photovoltaics. Her research interests include the modeling and simulation of power systems and electricity markets with a large penetration of renewable energy sources.