Sustainable Energy, Grids and Networks 28 (2021) 100549

Contents lists available at ScienceDirect

Sustainable Energy, Grids and Networks

journal homepage: www.elsevier.com/locate/segan

Precision timing and communication networking experiments in a real-time power grid hardware-in-the-loop laboratory

Prottay M. Adhikari [a,*], Hossein Hooshyar [b,*], Randall J. Fitsik [a], Luigi Vanfretti [a,*]

[a] Department of Electrical, Computer and Systems Engineering, Rensselaer Polytechnic Institute, Troy, NY, United States of America
[b] Electric Power Research Institute, White Plains, NY, United States of America

ARTICLE INFO

Article history:
Received 11 June 2021
Received in revised form 2 September 2021
Accepted 5 October 2021
Available online 12 October 2021

Keywords:
Power System Laboratory
Communication Protocols
GOOSE (IEC 61850) Protocol
GPS
C37.118 Protocol

ABSTRACT

The growing wave of digitization in power grids is bringing increased reliance on information and communication technologies (ICT) for the operation of the grid. Such cyber–physical power systems (CPPS) involve the interaction of the physics of the power grid with the performance of other engineered systems, such as communications and time-synchronization. To understand the interplay of such interactions, experimentation is required. However, there are very limited opportunities to perform experiments on *actual* CPPS systems, due to safety and security concerns. Nevertheless, the demand for more functionalities on cyber components will continue to rise, and thus, other means to understand CPPS behavior for design, implementation and testing are needed.

To address this gap, a real-time simulator-based power system laboratory was implemented with the objective of facilitating experiments involving precision timing and communication networking systems which are coupled with power grid models running in real-time. These are integrated in three layers: (a) Precise Timing Layer, (b) Communication/Network Layer, and (c) Electrical Component Layer. This paper reports on detailed experiments performed on the precision timing and communication layers of the laboratory. It shows how to couple the different layers together, and how to conduct experiments to tamper with both the precision timing and communication layers, along with their interactions with the simulated grid. Finally, the paper shows how to validate the Quality of Service (QoS) rules implemented in virtual local area networks (VLANs) in the laboratory environment when using different power system communication protocols.

1. Introduction

This section discusses the motivation behind this research and presents a brief literature review. Additionally, it enlists the specific contributions reported in this paper. Section 2 reviews the architectural details of the laboratory. Section 3, describes the experiments performed to demonstrate the cyber–physical interactions in the different layers of the laboratory, and summarizes the observations and results obtained from those experiments. The paper concludes with a summary of the current and prospective experimental research suitable for this kind of laboratory infrastructure.

1.1. Motivation

The digitization of power grid coupled with the penetration of various distributed non-conventional energy resources has led to a different paradigm of how a power system operates. This new paradigm reveals new challenges in the fields of monitoring, protection and communication in a power network. This has required the development of new capabilities on the "cyber" assets to address these challenges, for example, networking and controlling inverter-based resources (IBRs). These infrastructures has been standardized in [1]. However, there are limited opportunities to test these new functionalities before they are deployed into the power grid, which in turn limits the understanding of their interaction and impact on the grid's operation.

To verify and validate new technologies requires to perform tests in laboratory conditions, researchers and engineers need elaborate testing tools that would be able to mimic the behavior of a power system in real-time. This requirement makes the utilization of various real-time simulators (e.g. Opal-RT, RTDS, Typhoon HIL) relevant in context of power systems research as discussed in detail in [2]. While these high-end computing devices emulate the physical behavior of the power system, the extensive data communication network of a modern power system needs to be implemented or emulated separately [3]. The analog or digital signals generated through the real-time simulators need to

* Corresponding authors.
E-mail addresses: prottaymondaladhikari@gmail.com (P.M. Adhikari), h.hoosh@gmail.com (H. Hooshyar), fitsir@rpi.edu (R.J. Fitsik), luigi.vanfretti@gmail.com (L. Vanfretti).

https://doi.org/10.1016/j.segan.2021.100549
2352-4677/

Abbreviations

CPPS	Cyber–physical power systems.
VLAN	Virtual local area network.
PTP	Precise timing protocol
GPS	Global positioning system
GNSS	Global navigation satellite system
GOOSE	Generic object oriented substation events
PMU	Phasor measurement unit
cRIO	Compact reconfigurable input/output
IED	Intelligent electronic device
SV	Sampled Value
SGAM	Smart Grid Architecture Model
IRIG-B	Inter-range instrumentation group — Time Code Format B.

be transmitted through this network following specific protocols, like IEEE C37.118 [4] and IEC 61850 [5], in order to run experiments that would emulate a modern interconnected digitized power system. This makes the network configuration associated with power system experimentation crucial for the validity of the experiments.

With the electrical layer (consisting of real-time simulators) emulating power systems in real-time, it is important to illustrate how those simulation results can be interfaced, monitored and analyzed throughout the network. Moreover, in order to validate industry-grade physical equipment (e.g. substation equipment such as digital relays [6], photovoltaic inverters [6], etc.) within a laboratory environment, all simulations, analog signals and measurement data need to carry precise timing information as demonstrated in [7]. This paper aims to illustrate these different infrastructures are brought together within a fully functional digital power grid laboratory, and more importantly, how the precision timing and communication networking systems can be safely and lawfully "tampered" with by proposing and performing real-time experiments.

1.2. Related works

Simulation labs for power system research are becoming ubiquitous among major research institutions. Some important examples of such laboratories were reported in [8–13]. However, the focus has largely emphasized the capabilities of these implementations on grid simulation with some communication networking, leaving the precise timing infrastructure outside of their design considerations. Precision timing becomes critical when dealing with applications that require time-synchronization, such synchrophasor data applications and protective relaying. As reported in [14], the ALSET laboratory implementation features a separate timing layer into its hierarchy, making the implementation suitable for real-time experimentation on time-critical applications. This approach is similar to the one proposed in [15], where the authors hypothesized a functional block based architecture for validating and evaluating smart grid functionalities. On a similar note, the authors in [16] proposed a software driven flexible testbed for these applications. The architecture explored in the current paper was directly influenced by the Smart Grid Architecture Model (SGAM) proposed in [17], and it can be visualized along three distinct layers: (a) Precise Timing Layer, (b) Communication/Network Layer, and (c) Electrical Component Layer. More details on the specifications and implementations of these layers are illustrated on Section 2.

In related works, authors of [12] reported a full-scale laboratory implementation featuring synchronous generators, physical loads (both passive loads and active loads) and converters. This implementation also incorporated a high-power hybrid DC–AC type power system, for testing various smart grid applications. While this research made significant contributions towards the development of a standalone power systems laboratory with a fully operational networked supervisory control and data acquisition (SCADA) system, the network implementation was not tested for various relevant power system communication protocols and precision timing. Built upon the implementation reported in [14], the current work specifically focuses on the protocols, networking and timing infrastructures of a power system research laboratory. Thus, most of the efforts were targeted towards the development and verification of fully operational time-sensitive network suited for smart-grid instrumentation.

As reported in [18], the future smart control centers would be able to carry out data-driven analysis over networked devices to apply control actions on various power system components. To realize such an infrastructure in a laboratory environment, the network implementation must be robust and it must support various networking protocols without any hardware reconfiguration. The current work reports such an implementation and presents some relevant test-cases which utilize those networking protocols. Additionally, with the introduction of Phasor Measurement Units (PMUs) and synchrophasor technologies in the power system, incorporation of a precise timing source have become a critical infrastructure for power system monitoring and protection. To incorporate this into any cyber–physical power system laboratory, the devices and network within the laboratory environment must support the IEEE 1588 compliant Precise Time Protocol (PTP) as recommended in [19]. The survivability and compliance-testing performed in [20] also reported a time-synchronized interconnection. The GPS facilities incorporated within a power network needs to be *secured* in order to ensure immunity against malicious external attacks as reported by the authors in [21]. Such malicious attacks were studied in details, in the context of a real-time CPS, by the authors in [22] and [23]. To tackle these issues, the research presented in [24] proposed spectrum-sharing for wireless communication enabled smart grid functionalities. However, because the proposed implementation in ALSET lab utilizes wired ethernet connections instead of wireless networks, it has a comparatively safer communication infrastructure. Apart from PTP and synchrophasor (C37.118), the power system specific data transmission protocols, that are of crucial importance for this current paper are IEC 61850 (GOOSE and SV).

As reported by the authors in [25], the IEC 61850 can be utilized to transmit seven different types of messages, with varying speed. The fastest `type` of message-Generic Object Oriented Substation Events (GOOSE) messages, which utilizes the IEC 61850 protocol for message transmission, suitable for reporting substation events such as faults. On the other hand, Sampled Value (SV) data transmits continuous voltage and current measurements through the same IEC 61850 protocol, but at a lower speed. The C37.118 protocol, on the other hand, is dedicated for transmitting time-stamped data generated through phasor-estimation algorithms at a fixed reporting rate (i.e. 50/60, 100/120 packets per second). The proposed laboratory implementation supports all these protocols, including PTP, GOOSE, SV, Synchrophasor and still keeps a provision for generic TCP/IP based data transfer operations within the network. Authors in [26] and [27] presented significant architectural details of similar setups from the perspective of communication engineering. The study presented in [28] explored the quality-of-service rules for the communications setups under similar configurations.

In terms of experimentation, the large majority of the software used in real-time simulation labs consists of proprietary tools such as the ones reported by the authors in [2] and [8], both for device configuration as for modeling and simulation. In this work, devices are configured with software provided by SEL (*Quickset* and *Architect*), Opal-RT (*RT-LAB*), and National Instruments (*LabVIEW*). However, to conduct the research in this work, other developed within the lab were necessary. One such tool was *Khorjin* [29] which provides a IEEE C37.118.2 to IEC 61850-90-5 mapping and transformation for real-time synchrophasor data transfer. This software can be used to implement a time-synchronized hardware-based *Synchrophasor Synchronization Gateway* that can ingest and process real-time synchrophasor data from multiple PMU-streams as reported by the authors in [30]. In this research *Khorjin* and *SSG* were utilized to trace the latency of real-time synchrophasor data streamed by various protection devices connected in the ALSET lab communication network. All these software requirements are also summarized in Table 2. This summary provides a useful benchmark which can be compared against the similar surveys published in [31].

1.3. Contributions

The main contributions of this paper are:

- To present how an SGAM-defined architecture has been implemented for three fundamental layers.
- To provide examples of experiments designed to illustrate how the electrical layer, the network layer and the timing layer interact with each other while running tests on a power system model. The results of those experiments are presented therein.
- To demonstrate how a precision timing network can be safely and lawfully impaired and how the IEDs respond to timing tampering.
- To demonstrate how a data communication-network was impaired and how the IEDs respond to such impairments.
- To show how delay tracing can be performed using a time-synchronized hardware-based *Synchrophasor Synchronization Gateway* which utilizes a GPS source present on-board for timing analysis.
- To report on experimental tests performed to demonstrate the different virtual LAN (VLAN) networks' operation.
- To demonstrate how Quality of Service (QoS) rules are implemented on VLANs and to propose experiments to validate them.

2. Review of the ALSET infrastructure

The electrical component layer of the ALSET lab infrastructure contains IEDs, real-time simulators and controllers with Ethernet connectivity. This layer is self-explanatory as there were no additional ALSET-specific configurations required for this layer. Thus, this section only reviews and summarizes the precise timing layer and the communication/network layer.

2.1. Review of the precise timing layer

The architecture for the timing layer of the ALSET lab is illustrated in Fig. 2. The four antennas are placed on the roof of the building, which receive both Global Positioning System (GPS) and Global National Navigation System (GNNS) signals and forward it them to Satellite Synchronized network clocks (SEL-2488), and to a 1-to-16 GPS splitter placed within the laboratory. The SEL-2488 clocks have the capability to extract precise timing information from the GNSS signal and make it available in several formats, including pulse-per-second (PPS), modulated and unmodulated Inter-range Instrumentation Group (IRIG)-B signals for the IEDs in the lab to utilize. These IEDs include the Opal-RT simulators, different SEL Relays, a SEL RTAC, and the server computer. Devices which have in-built GPS receivers (e.g. NI-cRIOs) require the raw GPS signals instead of the IRIG-B signal. Thus, they are fed direct GPS signals from the GPS-splitter. LMR-400 coax cables were used for transmitting GPS signals and RG-58 coax cables were used to transmit IRIG-B signals. All the IEDs in the laboratory were configured to receive timing information externally via their IRIG-B inputs. It may be necessary to use additional DC blockers (e.g. MCL 15542) and attenuators (e.g. BW-VX-1W54) to keep the signal level of the GPS signal within the permissible limit specified by the IED that is receiving the GPS signal. These hardware adjustments were specifically utilized for connecting NI-cRIO devices to the ALSET timing network. On the other hand, Opal-RT simulators are synchronized through Oregano Systems syn1588® PCIe network cards. Fig. 1 demonstrates the user interface for the SEL-2488 substation clock, which displays its reception of the GPS and GLONASS signals from the satellites via the antennas. GLONASS signals were not used in the experiments reported in this paper.

2.2. Review of the communication network layer

The communication network layer consists of multiple virtual LAN (VLAN) implementations which are targeted for specific types of data-transmission. This configuration ensures that the path utilized by each type of data are *virtually separated* even though they share the same physical LAN hardware (consisting ethernet cables and network-switches). Since most of these data are time-critical and the latency needs to be minimized, the VLANs were configured with two pre-defined Quality-of-Service (QoS) rules. These two rules defined the priority with which a certain data type is issued a queue and the guaranteed minimum bandwidth (GMB) of that issued queue. A summary of the specifications for the five existing VLANs is presented in Table 1. The architecture of this layer is illustrated in Fig. 3.

More detailed descriptions of the timing layer and the network layer can be found in [14].

3. Experiments

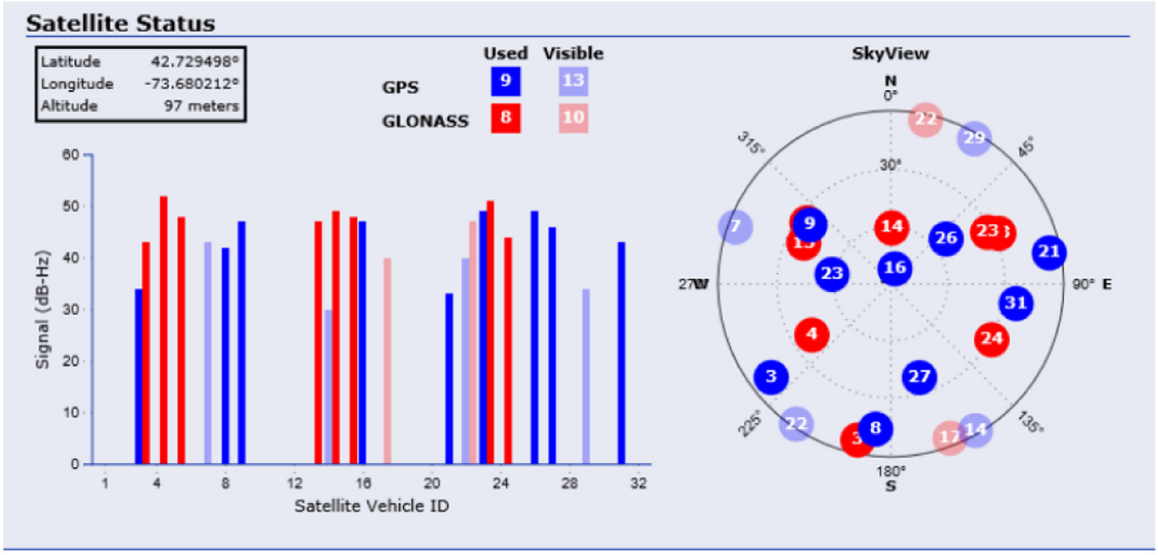
3.1. Experiment 1: Demonstration of the different VLAN data types

In this experiment various data types were transmitted within the ALSET-network and the streamed packets were captured and monitored through *Wireshark*. The actual data-content of the streams were kept minimal, so that visualization is easier and latency low. It can be observed in Fig. 4 that *Wireshark captures* display the VLAN ID and the corresponding priority for each data type. It can also be seen that each protocol has some data-bytes dedicated for identifying the source which that data is coming from.

Fig. 4 also illustrates that the GOOSE data was transmitted from SEL-421 relay with the appropriate VLAN tag. Since the available SEL-421 is not capable of transmitting SV-data, the representative SV-data were transmitted from OPAL-RT real-time simulator. The PTP-data represented in Fig. 4 was generated from a SEL-2488 Satellite Synchronized Networked clock.

3.2. Experiment 2: Demonstrating the three layers of ALSET lab through an experiment

This experiment illustrates how the three layers of the ALSET lab are interconnected and how they interact in the context of a simple experiment. The overall configuration, and a set of representative observations for this experiment is shown in Fig. 5.



Time Input

Available Sources	Time Quality
GPS (Selected)	**< 100 nsec**
Holdover	< 100 nsec
Local Time Offset:	-04:00
Daylight Saving Time Status:	Active
Daylight Saving Time Ends At:	2018-11-04T02:00:00-04:00

Time Output

Output	Format	Time Reference
TO1	IRIG-B004	UTC
TO2	IRIG-B004	UTC
TO3	IRIG-B004	UTC
TO4	IRIG-B004	UTC
TO5	IRIG-B004	Local
TO6	IRIG-B004	Local
TO7	IRIG-B004	Local
TO8	IRIG-B004	Local
COM1	IRIG-B004	Local
OUT1	Disabled	

Fig. 1. The source of timing information: As seen on the substation clock GUI.

Table 1
Specifications of the existing ALSET VLANs.

VLAN	VLAN ID	Priority	GMB	GMB of switch	Application
GOOSE	50	7	1 Mbps	Strict	Substation events (Breaker/Alarm)
PTP	40	6	5.2 kbps	1%	Precise timing information
SV	30	4	480 Mbps	50%	Instantaneous transmission of current/Voltage measurements
PMU	20	3	5 Mbps	1%	Synchrophasor measurements following C37.118
Station	10	0	100 Mbps	10%	Generic file operations (print-jobs, model-transfer)

Experiment configuration:

The electrical layer consists of an OPAL-RT real-time simulator which hosts a program that generates three phase analog voltages (0–0.5 V range) on its output pins. These analog signals are then connected to the SEL-421 relay's low voltage AMS interface through a IDC34P-B breakout board. The SEL-421 relay estimates the phasors corresponding to the analog voltages based on its internal CT and PT settings, and transmits those phasor measurements at a reporting rate of XY packets per second utilizing C37.118 protocol through the ALSET lab VLAN network. The NI cRIO hardware (connected to the same VLAN) uses the *Khorjin* package to decipher the data enclosed in the C37.118 protocol in real-time, and displays them over the GUI designed on LabVIEW. The uniqueness of this setup is, unlike traditional PDCs the cRIO hardware utilizes an on-board receiver for GPS signal, making the architecture suitable for timing-analysis and timestamp-tracing.

Experiment results:

This is how the network layer of the lab is utilized by an experiment in real-time. The cRIO, which runs the *Khorjin* package to unwrap the synchrophasor data, receives the GPS signal on the NI-9467 GPS module through the RMS-116 GPS splitter. The effective output of this experiment is dependent on the magnitude of the analog signals generated from the OPAL-RT Real-time simulator and the internal CT/PT settings of the SEL-421 relay. This output can be visualized on a LabVIEW based GUI proposed and designed by the authors in [29] and [30].

Possible adjustments for cost-reduction:

It is possible to run similar tests with a much simplified electrical layer. Instead of generating low-voltage analog signals from a real-time simulator, it can be possible to generate multiple sets of low-voltage analog signals using embedded microcomputer kits like *Raspberry Pi* or *Arduino*, and test the communication and timing infrastructures. Additionally, it is possible to replace the extensive Antenna-network of the reported laboratory, with low-cost USB GPS receivers. These adjustments will put a lot of geographical restraints on the setup, and make the system less flexible. However, they would reduce the cost of the system-development to a great extent.

3.3. Experiment 3: Tampering with the network layer

In this test the communication/network layer of the ALSET Lab is tampered with a communication network emulation device.

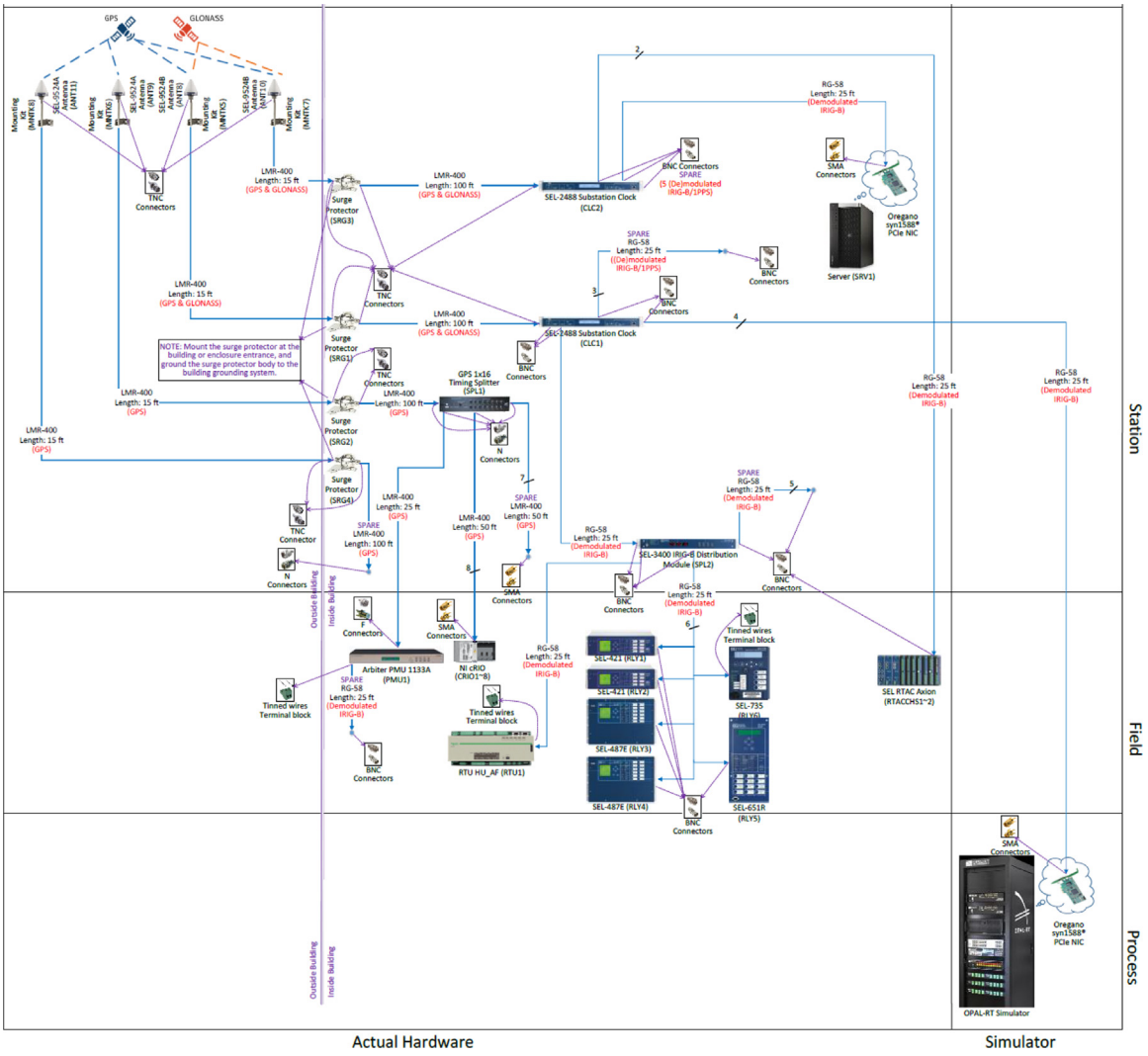


Fig. 2. Architecture of Timing Layer for the ALSET Lab.

Experiment configuration:

This device (*CT910* manufactured by *CandelaTech*) was placed between the SEL-421 Relay streaming synchrophasor data and the remaining ALSET lab network, and was configured to introduce a latency of 1000 ms. The SEL relay was fed analog three-phase voltages from the OPAL-RT real-time simulator. The same signals were fed to another SEL-421 Relay streaming synchrophasor data directly into the ALSET Lab network **without** the *CT910* network-tampering device in between. Both these synchrophasor streams were read in real-time on the NI cRIO running the *Khorjin* software. The voltage source that feeds analog inputs to the SEL-421s is easily configurable through Simulink. The experimental setup is illustrated in Fig. 6.

Experiment results:

A step change of 0.5 Hz was applied to the frequency of this source for a window of 1 s. This step-change in frequency is reflected in both the synchrophasor streams. Observe that due to the tampering, the step-change is shown 1000 ms apart because of the injected latency via the CT910. This allows to observe and quantify the tampering the network for one of the PMUs. This experimental observation was monitored in real-time on LabVIEW GUI and the results are logged and presented in Fig. 7. Notably, this setup enables the user to trace the network delay accurately by utilizing its on-board GPS module. The timestamp received through this GPS module can be compared with the time-stamp embedded in the PMU data-stream to compute the network delay.

3.4. Experiment 4: Tampering with the timing layer

Impairing the timing layer is more challenging because it is unlawful to tamper with GPS signals, and thus, it is not possible to directly affect the signal received by the GPS antennas. Hence, this section shows how timing can be safely and lawfully impaired for experimentation. The only lawful way to tamper with the precise timing layer is to generate an alternate source of timing signal in the IRIG-B format. The authors in [23] presented how mock IRIG-B signal can be generated through the output ports from the Opal-RT simulator. In this research, an IRIG-B signal was generated following the same technique.

Experiment configuration:

In this experiment, two different models were simulated on the OPAL-RT hardware. The first one generated low voltage analog signals as described in Experiment 3. The second model is used to generate dummy IRIG-B signals to one of Opal-RT's digital output ports. This port was connected to one of the SEL-421's IRIG-B input. Thus, this SEL-421 PMU does not have access to the satellite synchronized precise clock, but it reads time from a

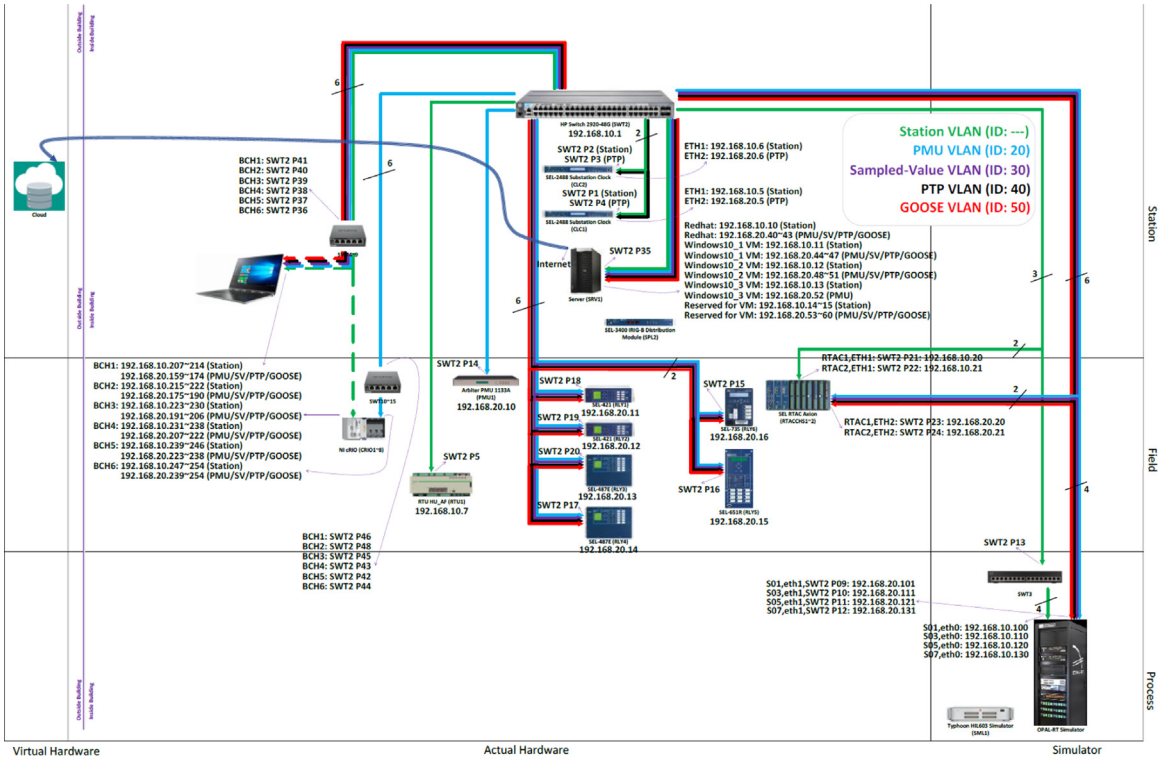


Fig. 3. Architecture of the Network Layer of the ALSET Lab illustrating all the Virtual LANs.

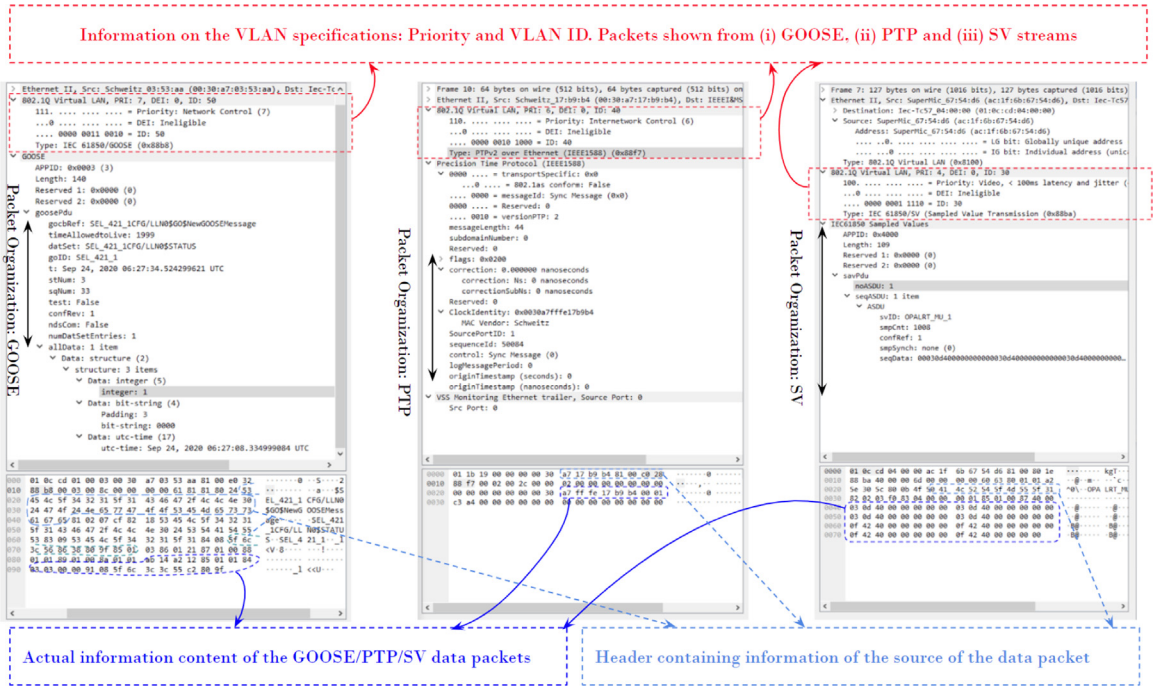


Fig. 4. Wireshark Screen Captures of the data packets through different VLANs implemented in ALSET Lab.

synthetic IRIG-B signal which is configured to represent a time in the year 2014. An example of such tampering is shown in Fig. 8. It can be seen in this figure that the tampered IRIG-B signal is translated into a wrong time from the year 2014, while the experiment was performed in March of 2021. The configuration of the overall experiment is shown in Fig. 9. Both the actual and corrupt IRIG-B signals are represented in light blue lines, and the PMU streams traveling through VLAN-network is represented in dark blue lines. The electrical part of this experimental setup, which generates the analog voltage signals is represented by red lines.

Experiment results:

The two synchrophasor streams would still read the same voltage signals with the exact same magnitude and frequency.

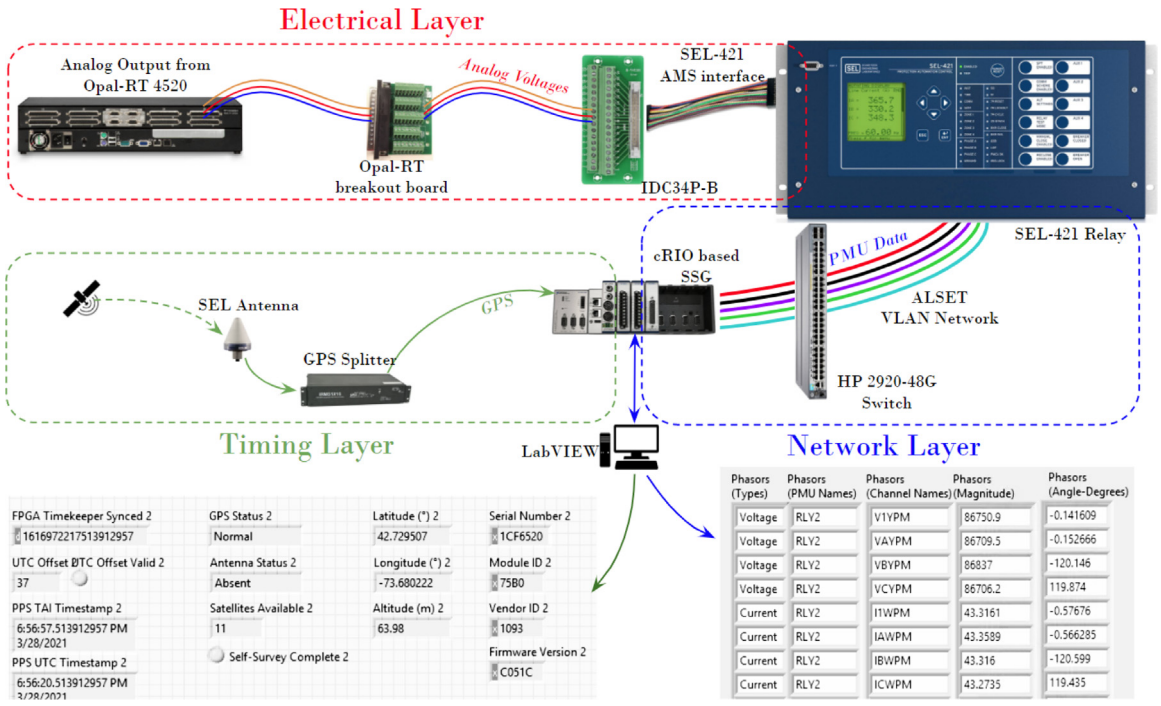


Fig. 5. Illustration of a simple real-time experiment that utilizes all three layers of the ALSET Lab hierarchy.

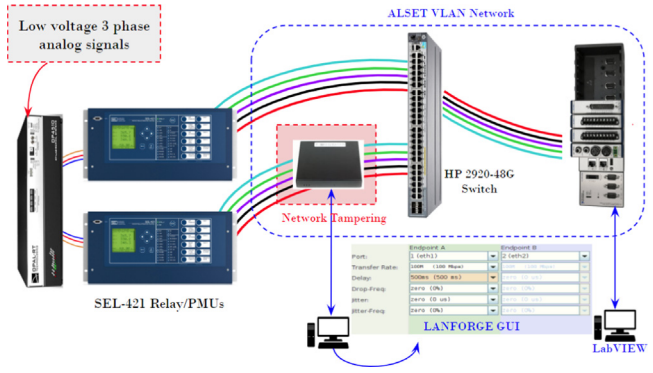


Fig. 6. Experimental setup to tamper with the network layer of the ALSET Lab.

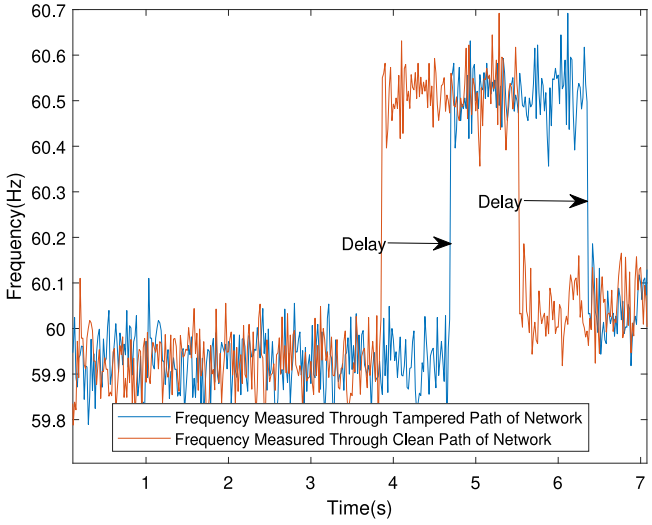


Fig. 7. Tracking the frequency of the synchrophasor data received through a tampered network.

However, since the timing-source of one of the streams is corrupted, it will fail to compute the phasor-angles correctly, as shown in Fig. 10.(a) while Fig. 10.(b) presents the correct phasor measurements from the SEL-421 relays.The GUI used for monitoring these measurements in real-time was implemented in LabVIEW. The phase angle mismatches can be observed directly on this GUI.

3.5. Experiment 5: Validating the QoS rules for the network

The QoS rules configured for the VLANs are verified in this experiment. These rules were first introduced in [14] and based on those rules the priorities and guaranteed minimum bandwidths (GMB) were specified. Two different experiments were performed to validate the QoS rule related to the priorities of the VLAN networks, and to validate the Guaranteed Minimum Bandwidth of those networks, respectively.

3.5.1. Experiment 5(a): Validating the QoS for priorities of VLANs:

It can be seen from Table 1, that GOOSE and PMU VLANs consume a similar range of bandwidth, but with different priorities. The objective of this experiment is to validate the priorities between these two VLAN networks.

Experiment configuration:

The network is utilized to transmit both PMU and GOOSE data initially. By using the functionalities provided by *CandelaTech Lanforge*, the total bandwidth of the network was then reduced from 1 Gbps to 256 Kbps, and the priority with which the two data-types were handled was monitored. The experimental setup is shown in Fig. 12.

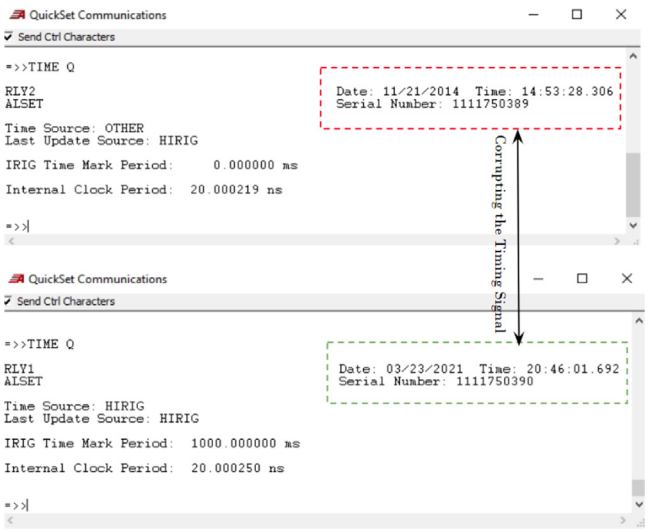


Fig. 8. Observing the corrupted timestamp of SEL-421.

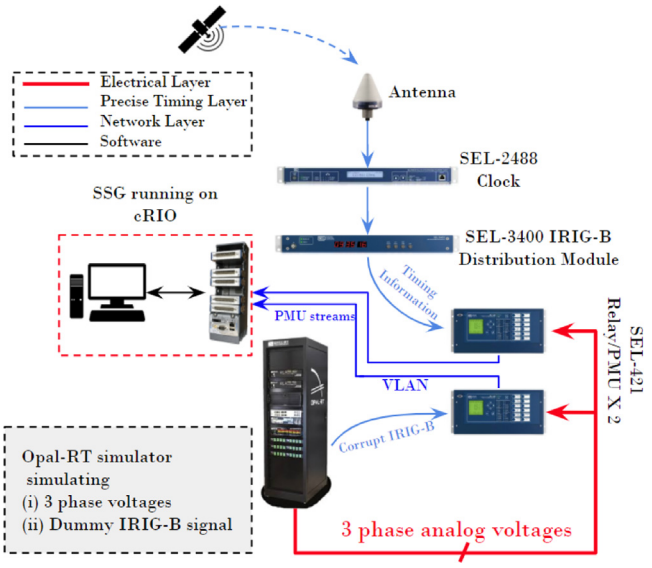


Fig. 9. Experimental setup to tamper with the precise timing layer of the ALSET Lab.

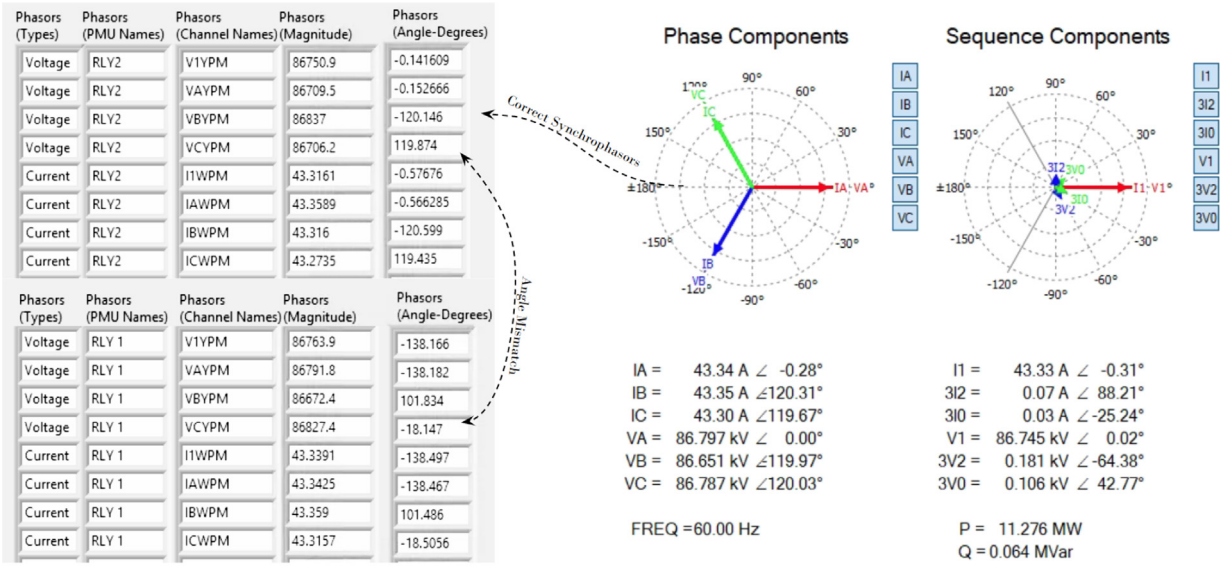
Experiment results:

The experimental protocol for this test can be divided into 2 phases as described below, along with the obtained results.

- **Phase 1:** Phase 1 spans from the initiation, up to 400 s as shown in Fig. 11. During this time, PMU and GOOSE data are streamed through the same channel utilizing different VLAN specifications. The bandwidth of the channel is the maximum possible bandwidth of the network, i.e. 1 Gbps. Under this operating condition, all the GOOSE and PMU packets will be successfully transmitted through the network. However, since the PMU message frames contain more bits than the GOOSE message frames, it can be seen that the majority of bandwidth is being utilized for transmitting PMU data (green plot).
- **Phase 2:** Phase 2 spans from the end of phase 1 (i.e. around 400 s) to 800 s as shown in Fig. 11. At the end of Phase 1, the bandwidth of the network was reduced to 256 Kbps by utilizing the *Lanforge Manager* software package. It can be seen from Fig. 11 that upon the imposition of this bandwidth restriction, the data-transfer through the PMU VLAN was drastically reduced, even though the data-transfer through the GOOSE VLAN was unaffected. This observation demonstrates that the GOOSE VLAN has a higher priority according the proposed QoS, and thus GOOSE transmissions are prioritized over PMU ones.

3.5.2. Experiment 5(b): Validating the guaranteed minimum bandwidth for the VLANs:

It is demonstrated in Table 1, that all VLAN networks have certain guaranteed minimum bandwidths. This means that even when there are higher priority data waiting in the queue, the data with lower priority VLAN would still be guaranteed a minimum



(a) Correct(above) and corrupted Synchrophasor Measurement from the NI-cRIO

(b) Representative correct synchrophasor measurement from the SEL-421

Fig. 10. Experimental Synchrophasor observation after tampering the timing layer.

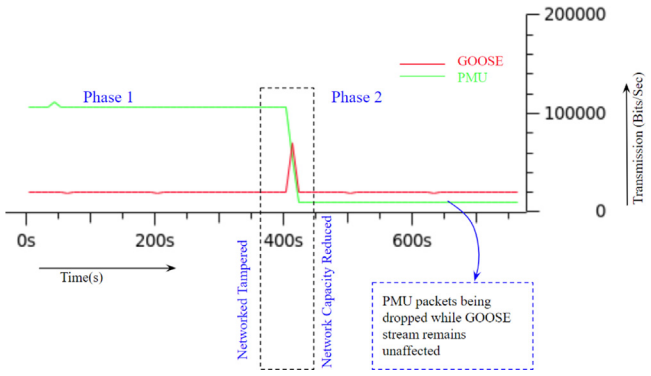


Fig. 11. Effect of the QoS priority rule, under varying network bandwidth.

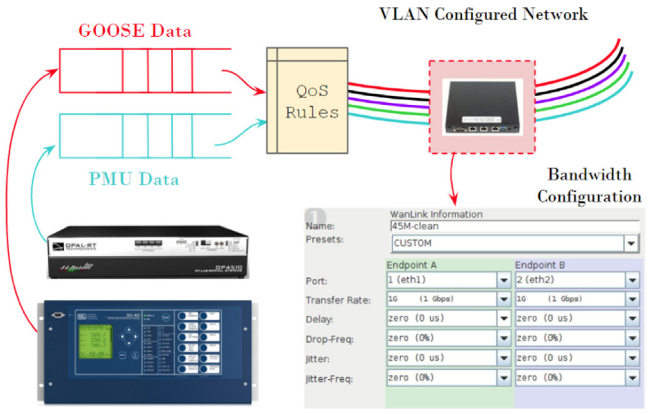


Fig. 12. Experimental setup to demonstrate the QoS rules.

bandwidth so that it does not get starved by the higher priority data. This experiment demonstrates the effect of this *minimum* bandwidth in data transmission through the ALSET network.

Experiment configuration:

For this experiment, the SEL relay and the PMU are configured to stream GOOSE and PMU streams in parallel. In this situation, the network's maximum capacity is set at 64 Kbps. Initially, this bandwidth is large enough to accommodate both these streams. However, the GOOSE data-load is increased by modifying the GOOSE-data packet's configuration from the SEL *AcSELerator Architect* software, twice at t = 200 s and t = 600 s, and then the observations are noted.

Experiment results:

The experimental observations for this test can be divided into 3 phases as described below, along with the obtained results.

- **Phase 1:** From t = 0 s to 200 s in Fig. 13, both PMU data and GOOSE data are streamed in parallel. The networks bandwidth of 64 Kbps was large enough to stream both these data-streams without any issues.
- **Phase 2:** This duration begins at 200 s and lasts till 600 s in Fig. 13. At t = 200 s, the load for GOOSE-data is increased. To incorporate this increased load of GOOSE stream within the same network of 64 Kbps capacity, the PMU data-stream reduced its transmission rate. This is because GOOSE VLAN has higher priority and the network has low bandwidth.
- **Phase 3:** This duration begins at 600 s and lasts till the end of this experiment as shown in Fig. 13. At t = 600 s, the GOOSE-data load is increased furthermore. Since, bandwidth is still kept constant at 64 Kbps, it was expected that the PMU transmission would reduce furthermore compared to what was observed in phase 2. However, the PMU VLAN transmission remained unaffected, even though the GOOSE transmission was increased. This can be explained by the fact that the PMU VLAN was operating at its *guaranteed minimum bandwidth*, so it would not operate at a lower bandwidth, even though there were higher-priority GOOSE data on queue.

3.6. Analysis and synthesis of experimental complexity:

The authors' experience in conducting these experiments reveals that while it is possible to conduct CPPS experiments safely and securely in the implemented laboratory setting, all technologies involved make the experimental configuration process time-consuming and hard to automate. In addition, there is a steep learning curve to master all the "cyber" know-how together with power grid understanding. This poses a major challenge for verification, testing and validation of cyber-components and systems that need to be deployed in the power grid to support the on-going energy transition. More efforts are needed in making experimental testing more efficient and reproducible to keep up with the rate of innovation in new functionalities being developed in the "cyber" side so to facilitate, not only their adoption without unwanted consequences, but also for the "physical" side to fully exploit the benefits of increased digitization. It needs to be noted that, the experiments demonstrated in this research required expensive equipment such as industrial relays, real-time simulators, and NI cRIOs. Additionally, the auxiliary infrastructures (e.g. arrangement of LMR cables, proper connection of GNC cable to attenuate/amplify the signal level, placement

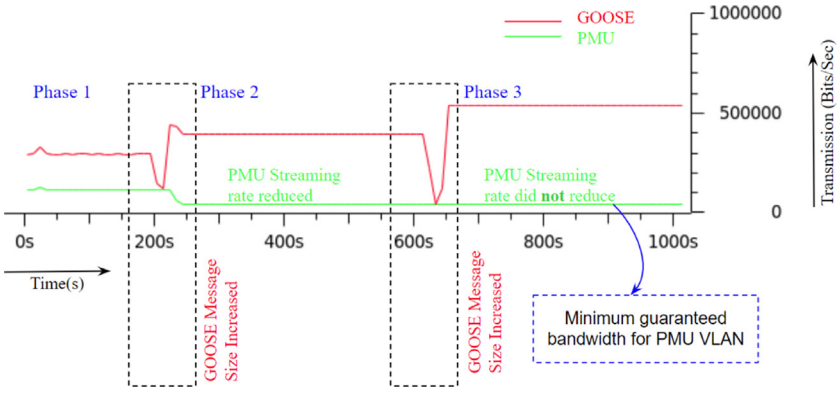


Fig. 13. Effect of the QoS guaranteed minimum bandwidth rule under varying GOOSE-data stream.

Table 2
Review of the complexity of the performed experiments.

Expt	Objective	Complexity	Software requirement	Hardware requirement	Comments
1	Validating the VLANs	Low	WireShark, SEL Quickset	SEL-421/Opal-RT	Source of the data varies based on VLAN choice
2	Introducing the 3 layers of the lab	Medium	RT-Lab, WireShark, LabVIEW	Opal-RT Simulator, NI-cRIO, Antenna	
3	Tampering communication Network	Medium	RT-Lab, Lanforge, LabVIEW	Opal-RT, CT-910, NI-cRIO	
4	Tampering timing network	High	RT-Lab, SEL Quickset, LabVIEW	Opal-RT Simulator, SEL-421, NI-cRIO, Antenna	Additional GNC cable needed
5(a)	Demonstrating the QoS rule-a	High	RT-Lab, SEL Quickset, Lanforge, LabVIEW,	Opal-RT, CT-910, SEL-421, NI-cRIO	The network bandwidth needs to be carefully
5(b)	Demonstrating the QoS rule-b	High	RT-Lab, SEL Quickset, Lanforge, LabVIEW, SEL Architect	Opal-RT, CT-910, SEL-421, NI-cRIO	Configured by Lanforge for each run.

of antennas) take significant amount of time to procure, deploy and setup. In an attempt to formalize, synthesize and grade the challenges involved in the experiments reported in this paper, the experiments were classified into three categories based on their complexity in Table 2. It is noteworthy to mention that, the proposed experiments are only designed to demonstrate the functionalities of the laboratory. An experiment to simulate and test real-world power system problems (as demonstrated in [13, 32]) increases complexity.

4. Conclusions

This paper reported the design and results from experiments of the precision timing and communication network layers of a cyber–physical power system simulation lab implemented at Rensselaer Polytechnic Institute. The experiments demonstrate how these two layers can be safely and lawfully tampered with, which can allow to better understand the interactions between different engineered systems of a cyber–physical power grid. Additionally, the VLAN network and its corresponding QoS rules were demonstrated by streaming predetermined set of data.

The results of the experiments reported in this paper validate the proposed SGAM-based architecture for digital power system simulation labs in [14]. While more extensive laboratories targeted for similar experiments exist in U.S. National Labs [8] and the industry [33], most of those implementations are too expensive and/or complex for most research/academic purposes. The implementation proposed in this work requires less resources and is suitable for teaching and training students and engineers alike. Section 3.2 proposed some major simplifications on the existing architecture, which can reduce the cost of the implementation drastically. The proposed simplifications however, are only valid for demonstrations at the lab scale because of the restrictive nature of the low-cost equipment. This implies that all the experimental demonstration on such low-cost systems would ultimately need to go through the expensive product development process before they can actually be utilized in a real-world grid setting.

CRediT authorship contribution statement

Prottay M. Adhikari: Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing – original draft, Approval of the version of the manuscript. **Hossein Hooshyar:** Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing – review & editing, Approval of the version of the manuscript. **Randall J. Fitsik:** Conception and design of study. **Luigi Vanfretti:** Conception and design of study, Analysis and/or interpretation of data, Writing – review & editing, Approval of the version of the manuscript.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This research was funded in part by the New York State Energy Research and Development Authority (NYSERDA), United States under agreement numbers 137948, and 149165; in part by the Engineering Research Center Program of the National Science Foundation and the Department of Energy under Award EEC-1041877, in part by the CURENT Industry Partnership Program, in part by the Center of Excellence for NEOM Research at King Abdullah University of Science and Technology, Saudi Arabia, and in part by Dominion Energy.

References

[1] IEEE Guide for Design, Operation, and Integration of Distributed Resource Island Systems with Electric Power Systems, available at https://standards.ieee.org/standard/1547_4-2011.html.
[2] X. Guillaud, et al., Applications of real-time simulation technologies in power and energy systems, IEEE Power Energy Technol. Syst. J. 2 (3) (2015) 103–115, http://dx.doi.org/10.1109/JPETS.2015.2445296.
[3] M.H. Syed, et al., Real-time coupling of geographically distributed research infrastructures: Taxonomy, overview, and real-world smart grid applications, IEEE Trans. Smart Grid 12 (2) (2021) 1747–1760, http://dx.doi.org/10.1109/TSG.2020.3033070.
[4] IEEE Standard for Synchrophasor Measurements for Power Systems available at https://standards.ieee.org/standard/C37_118_1-2011.html.
[5] Communication networks and systems for power utility automation – Part 1: Introduction and overview, available at: https://webstore.iec.ch/preview/info_iec61850-1%7Bed2.0%7Db.pdf.
[6] M.S. Almas, L. Vanfretti, RT-HIL implementation of the hybrid synchrophasor and GOOSE-based passive islanding schemes, IEEE Trans. Power Deliv. 31 (3) (2016) 1299–1309, http://dx.doi.org/10.1109/TPWRD.2015.2473669.
[7] Time Synchronization in Electric Power Systems, NASPI Technical Report, 2017, Available at: https://www.naspi.org/sites/default/files/reference_documents/tstf_electric_power_system_report_pnnl_26331_march_2017_0.pdf.
[8] M.H. Syed, et al., Real-time coupling of geographically distributed research infrastructures: Taxonomy, overview, and real-world smart grid applications, IEEE Trans. Smart Grid 12 (2) (2021) 1747–1760, http://dx.doi.org/10.1109/TSG.2020.3033070.
[9] M.J. Turner, Design and development of a smart grid laboratory for an energy and power engineering technology program, Int. J. Electr. Eng. Educ. 54 (4) (2017) 299–318, http://dx.doi.org/10.1177/0020720916687315.
[10] Distributed Electrical Systems Laboratory Available at: https://www.epfl.ch/labs/desl-pwrs/research/. Last Accessed on Feb '21).
[11] A.M. Gaouda, A. Abd-Rabou, A. Dahir, Developing educational smart grid laboratory, in: Proceedings of 2013 IEEE International Conference on Teaching, Assessment and Learning for Engineering, TALE, Bali, Indonesia, vol. 2013, 2013, pp. 404–409, http://dx.doi.org/10.1109/TALE.2013.6654471.
[12] V. Salehi, A. Mohamed, A. Mazloomzadeh, O.A. Mohammed, Laboratory-based smart power system, part I: Design and system development, IEEE Trans. Smart Grid 3 (3) (2012) 1394–1404, http://dx.doi.org/10.1109/TSG.2012.2194518.

[13] F. Huerta, J.K. Gruber, M. Prodanovic, P. Matatagui, T. Gafurov, A laboratory environment for real-time testing of energy management scenarios: Smart energy integration lab (SEIL), in: 2014 International Conference on Renewable Energy Research and Application, ICRERA, vol. 2014, 2014, pp. 514–519, http://dx.doi.org/10.1109/ICRERA.2014.7016438.

[14] H. Hooshyar, L. Vanfretti, J.H. Chow, R. Fitsik, P.M. Adhikari, ALSET lab: Designing precise timing and communications for a digital power grid laboratory, in: 2020 IEEE Power & Energy Society General Meeting, PESGM, Montreal, QC, Canada, vol. 2020, 2020, pp. 1–5, http://dx.doi.org/10.1109/PESGM41954.2020.9281808.

[15] C. Landsteiner, F. Andren, T. Strasser, Evaluation and test environment for automation concepts in smart grids applications, in: 2011 IEEE First International Workshop on Smart Grid Modeling and Simulation, SGMS, Brussels, Belgium, vol. 2011, 2011, pp. 67–72, http://dx.doi.org/10.1109/SGMS.2011.6089200.

[16] H. Tong, M. Ni, L. Zhao, M. Li, Flexible hardware-in-the-loop testbed for cyber physical power system simulation, IET Cyber-Phys. Syst. Theory Appl. 4 (2019) 374–381, http://dx.doi.org/10.1049/iet-cps.2019.0001.

[17] Smart Grid Coordination Group Smart Grid Reference Architecture, CEN-CENELEC-ETSI, Technical Report, 2012.

[18] P. Zhang, F. Li, N. Bhatt, Next-generation monitoring, analysis, and control for the future smart control center, IEEE Trans. Smart Grid 1 (2) (2010) 186–192, http://dx.doi.org/10.1109/TSG.2010.2053855.

[19] Andrea Carta, Nicola Locci, Carlo Muscas, Fabio Pinna, Sara Sulis, GPS and IEEE 1588 synchronization for the measurement of synchrophasors in electric power systems, Comput. Stand. Interfaces (ISSN: 0920-5489) 33 (2) (2011) 176–181, http://dx.doi.org/10.1016/j.csi.2010.06.009.

[20] Miguel Correia, Jorge Sousa, Álvaro Combo, António P. Rodrigues, Bernardo B. Carvalho, António J.N. Batista, Bruno Gonçalves, Carlos M.B.A. Correia, Carlos A.F. Varandas, Implementation of IEEE-1588 timing and synchronization for ATCA control and data acquisition systems, Fusion Eng. Des. (ISSN: 0920-3796) 87 (12) (2012) 2178–2181.

[21] C. Bonebrake, L. Ross O'Neil, Attacks on GPS time reliability, IEEE Secur. Priv. 12 (3) (2014) 82–84, http://dx.doi.org/10.1109/MSP.2014.40.

[22] C. Konstantinou, M. Sazos, A.S. Musleh, A. Keliris, A. Al-Durra, M. Maniatakos, Gps spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment, IET Cyber-Phys. Syst. Theory Appl. 2 (2017) 180–187, http://dx.doi.org/10.1049/iet-cps.2017.0033.

[23] M.S. Almas, L. Vanfretti, R.S. Singh, G.M. Jonsdottir, Vulnerability of synchrophasor-based WAMPAC applications' to time synchronization spoofing, IEEE Trans. Smart Grid 9 (5) (2018) 4601–4612, http://dx.doi.org/10.1109/TSG.2017.2665461.

[24] M. You, Q. Liu, H. Sun, New communication strategy for spectrum sharing enabled smart grid cyber–physical system, IET Cyber-Phys. Syst. Theory Appl. 2 (2017) 136–142, http://dx.doi.org/10.1049/iet-cps.2017.0051.

[25] Mohd. Asim Aftab, S.M. Suhail Hussain, Ikbal Ali, Taha Selim Ustun, IEC 61850 based substation automation system: A survey, Int. J. Electr. Power Energy Syst. (ISSN: 0142-0615) 120 (1850) 106008.

[26] Y. Wu, L. Nordström, Adaptive data link configuration for WAMC applications using a stateful data delivery service platform, Sustain. Energy Grids Netw. 6 (2016) 166–175, http://dx.doi.org/10.1016/j.segan.2016.04.001.

[27] E. Tebekaemi, D. Wijesekera, Secure overlay communication and control model for decentralized autonomous control of smart micro-grids, Sustain. Energy Grids Netw. 18 (2019) 100222, http://dx.doi.org/10.1016/j.segan.2019.100222.

[28] A. Alvarez de Sotomayor, D. Della Giustina, G. Massa, A. Dedè, F. Ramos, A. Barbato, IEC 61850-based adaptive protection system for the MV distribution smart grid, Sustain. Energy Grids Netw. 15 (2018) 26–33, http://dx.doi.org/10.1016/j.segan.2017.09.003.

[29] S.R. Firouzi, L. Vanfretti, A. Ruiz-Alvarez, F. Mahmood, H. Hooshyar, I. Cairo, An IEC 61850-90-5 gateway for IEEE C37.118.2 synchrophasor data transfer, in: 2016 IEEE Power and Energy Society General Meeting, PESGM, Boston, MA, USA, 2016, pp. 1–5, http://dx.doi.org/10.1109/PESGM.2016.7741393.

[30] P.M. Adhikari, L. Vanfretti, Delay analysis of a real-time hard reconfigurable synchrophasor synchronization gateway, in: Presented at the Control and Optimization of Renewable Energy Systems, 2019, http://dx.doi.org/10.2316/p.2019.859-008.

[31] Kai Heussen, Oliver Gehrke, Holger Kley, Anna Magdalena Kosek, Anders Thavlov, Use Cases for Laboratory Software Infrastructure - Outline of Smart Grid Lab Software Requirements, Report Number: D2, Technical University of Denmark.

[32] T. Becejac, C. Eppinger, A. Ashok, U. Agrawal, J. O'Brien, PRIME: a real-time cyber–physical systems testbed: from wide-area monitoring, protection, and control prototyping to operator training and beyond, IET Cyber-Phys. Syst. Theory Appl. 5 (2020) 186–195, http://dx.doi.org/10.1049/iet-cps.2019.0049.

[33] AGILe lab, 2021, available at: https://www.nypa.gov/innovation/digital-utility/agile-lab . (Last Accessed: 2021).