A SDN Based Method for Blocking Malicious Attacks on Digital Substations Communication

Santiago Sanchez-Acevedo, Salvatore D'Arco
Department of Energy Systems
SINTEF Energy Research
Trondheim, Norway
Email: santiago.sanchez@sintef.no

***Abstract*—IEC 61850 is the present standard recommended for the power system substations. The transition to IEC 61850 challenges the classical approaches of substation engineers especially regarding ensuring a high level of trustfulness in the communication. This paper presents a method for detecting and blocking the injection of malicious or replicated messages in a digital substation. This addresses both sampled values and GOOSE packets. Moreover, an example of implementation is presented and validated on an experimental setup replicating the behavior of a digital substation.**

***Index Terms*—Digital Substations, GOOSE Messages, Sampled Values, Cybersecurity.**

I. Introduction

Digital substations (DiSt) represent the evolution of the electrical substations. Control and protection devices were interconnected with copper cables. But, now those devices are replaced with Intelligent Electronic Devices (IED) with fiber optic network. This new way to monitor, control and protect the electric power system represents a cyber-physical system (CPS). Moreover, the power system infrastructure and the information and communication technology are known as cyber-physical power system (CPPS).

To test and validate new protection functions and devices of a DiSt it is important to count with a testbed. Literature of a DiSt laboratory setup is presented in [1]. Artificial substation traffic has been presented in [2], [3]. A setup for distance protection with multi-vendor IEDs is reported in [4].

Protection against cyber-attacks of the DiSt is imperative. Therefore, it is necessary to develop tools like intrusion detection system (IDS) that keeps the DiSt free of malicious data. As reported in [5], it is a big challenge to get a database for training and testing IDS or intrusion detection and prevention system (IDPS) for process bus traffic based on multicast sampled value (SV) or generic object oriented substation event (GOOSE) protocols. This paper addresses this issue using the Norwegian Smart Grid laboratory's substation testbed reported in [6]. The test-bed is equipped with state-of-the-art technology that can be used for testing cyber-security vulnerabilities of power substation configurations. Some examples of attacks are defined in [7], [8].

This paper was developed within the EU project SDN-microSENSE founded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 833955 and the Norwegian national project ECODIS founded by the Research Council of Norway project number 296550.

In a CPPS communication, control and computation technologies are critical for proper operation. Besides, it was demonstrated in smart grids that catastrophic effects can occur if the CPPS is exposed to attacks on the communication, control and computation infrastructure. The authors in [7] define CPPS cyber-attacks as 'those which are conducted on power system or power resources for the purpose of destroying or reducing functions of CPPS by tracking the behaviours of communication and control systems in an disallowed situation, and exploiting security loopholes and defects of communication network'.

The attacks on the DiSt's process bus can be deployed by multiple types of sources as summarized in [5]. An attacker gets access to the substation network. The source of attack could be installing malware in the device or infecting other devices in the DiSt network. This paper assumes the attacker reached the process bus of the DiSt.

a) Replay attack: A replay attack is based on re-sending previous messages that have been presented in the station flow. In this frame of attack, an attacker captures and replays the message without modifying the content [5]. Authors in [5], [9] recommend to check the timestamp and sequence number of the packets to detect this malicious behavior.

b) Message injection: This attack sends malicious packets with false values. Message injection attack can craft or modify the packet to be consistent with the rules of IEC 61850. In this technique packets are modified or built instead of only replayed.

Main contribution: To the best of authors' knowledge, the online IDPS system of process bus in a substation with software defined network (SDN) control architecture has not been previously presented. Moreover, the authors present a CPS testbed for validation of cyber-security methodologies in digital substations.

This paper is organized as follows: Section II describes the basic configuration for digital substations with IEC-61850. Section III presents the intrusion detector system. Section IV shows the testbed used for validation of the IDPS and section V presents the experimental validation of the IDPS based on

software define networks. Finally, section VI highlights the conclusions of the paper.

II. Station configuration based on IEC-61850

IEC 61850 standard is recommended for substation applications. It presents an object oriented structure that facilitates the modeling. IEC 61850 communication standard defines sampled values, GOOSE and MMS client-server as protocols to handle data exchange between the devices used in the substation.

a) Hardware of the digital substation: the intelligent electronic device is defined as a device featuring versatile electrical protection functions, advanced local control intelligence, monitoring abilities and the capability of extensive communications to a SCADA system [10]. In the substation based on IEC61850 the current and voltage measured are digitized with merging unit (MU) and their values transferred based on the IEC 61850-9-2 at the process bus. Hence, IED or other devices subscribe to MUs. Finally, network switches are used to control the traffic at process bus between MU and IEDs.

III. Substation monitoring application, intrusion detection and prevention system

This section presents first a customized application that is used for monitoring sampled values and GOOSE packets. Second part of this section describes the IDPS developed for removing cyber-attacks for multicast packets of IEC61850.

A. Monitoring application

A graphical user interface (GUI) application has been developed based on the open source library for IEC 61850 [11]. The GUI has been developed in Python and it maps the packets obtained with the IEC61850 library based on C to Python. Hence,the GUI is used for monitoring the selected sampled values or GOOSE destination addresses. This GUI is used only as a monitoring tool for the intrusion detection system. Therefore, alarms can be visualized by the system operator or as human machine interface at DiSt.

B. Resilient digital substation concept

The aim is to allow the substation to self heal in case a malicious or bad packet is detected for SVs or GOOSE. The intrusion detection and prevention system developed in this paper is structured as shown in Fig. 1. The IDPS described in this paper uses three components. First stage uses a detector based on the first derivative of the sequence numbers for SVs or GOOSE packets. A database logic module (DBM) compares the connection ports of the substation devices with the identified possible flow attack. Finally, in Fig. 1 an SDN controller receives the action flow and configures the SDN switch to remove the attacker.

The event detector has been developed based on the first derivative of the online monitoring variables. Equation (1) shows the differential function used on the detector. The

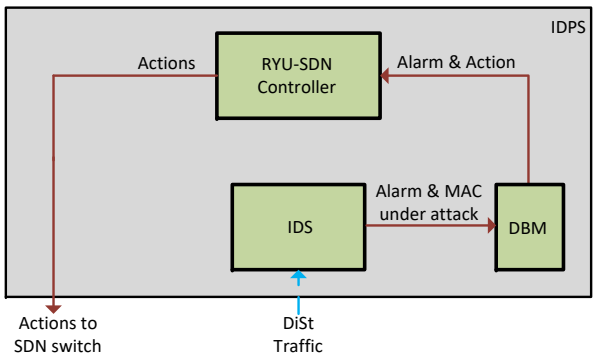

Fig. 1. Architecture of the intrusion detection and prevention system. Intrusion detection system (IDS), database logic module (DBM) and intrusion detection and prevention system (IDPS).

monitoring variable x can be the sequence ($SeqNum$) and state ($StNum$) numbers for GOOSE or the sample counter ($smpcnt$) for SVs, respectively. The event detection is the IDS presented in Fig. 1.

$$diff(x) = x_k - x_{k-1} \tag{1}$$

The steps used in the event detector that identifies the attack are summarized in the pseudocode indicated as Algorithm 1. Variable $Alarm_{GOOSE}$ is an alarm for GOOSE message, alarm for SVs is $Alarm_{SV}$. Threshold number (thr) tunes the detector. Hence, IDS uses $thr = 2$. Finally, if alarms of IDS for the monitored MAC address is activated, the MAC address information is loaded to the database with the alarm.

Algorithm 1 Steps for the IDS of DiSt

procedure IDS(DiSt Traffic)
$Alarm_{GOOSE} \leftarrow thr < diff(x)\ \forall x \in \{SeqNum, StNum\}$
$Alarm_{SV} \leftarrow thr < diff(smpcnt)$
if $Alarm_{GOOSE} == 1\ ||\ Alarm_{SV} == 1$ **then**
Write MAC information
return $Alarm\ \&\ MAC$

Once the attack has been detected the information from IDS goes to DBM. DBM compares the allowed topology of the substation. DBM uses the MAC address to collect information from a database of the substation publishers. Hence, the DBM logic finds which ports in the substation are not allowed to publish with this MAC. The DBM server sends the list of ports to block with the SDN controller in the substation's SDN switch. Finally, the SDN controller uses a client to monitor any action written by the DBM server. The client at the SDN controller passes the list of action flows to write from the controller to the substation's SDN switch. In this work the SDN controller is the open source RYU controller.

IV. Testbed implementation

The testbed shown in Fig. 2 describes a cyber-physical power system testbed and it is based on a hardware-in-the-loop

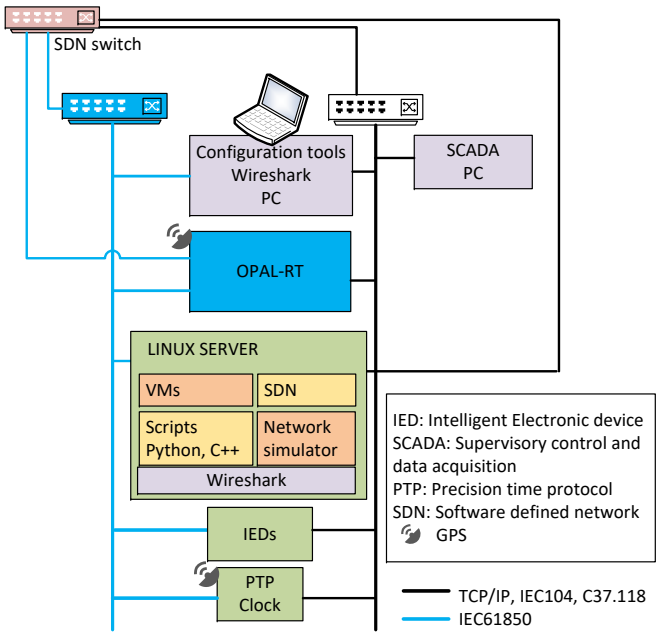

Fig. 2. Overview of the testbed for cyber-physical power systems at the Norwegian National Smart-Grid laboratory.

architecture. The system has a real-time simulator for emulating the dynamics of the electric power system. In addition, the real-time (RT) simulator has smart grid communication protocols to communicate with real field devices. This testbed uses as field devices an industrial IED, a network clock based on GPS synchronization, power system communication switches, one SDN switch, an industrial SCADA and a linux server for implementing scripts or network monitoring. Blue line in Fig. 2 represents the multicast traffic based on standard IEC 61850. Black line is used for traffic for smart grid protocols based on TCP/IP such as IEC 60870-5-104 (IEC104) and C37.118.

RT simulation is used for representing the electric transient dynamic of the distribution substation. A digital real-time simulator from OPAL-RT is used for developing the electric power grid and monitoring of physical devices. Additionally, the OPAL-RT platform uses communication protocols such as IEC 61850, IEC104, DNP3, and C37.118. These protocols allow the simulator to interact at all levels of the SCADA architecture, process and station buses.

The real-time simulator is used as a MU for the voltage and currents in DiSt. RT simulator can be used for subscribing and storing the GOOSE messages and SVs traffic in DiSt network. The SDN switch controls the traffic of packets in the DiSt at process and station buses.

V. Experimental Validation

Previous sections presented the core of components that are part of the hardware and the components that are accessed via software interfaces like the IT devices. This section presents an application of the components of the CPPS testbed. The experiment analyzes the behaviour of the undervoltage protection function of an IED. Besides, the experiment demonstrates the effects of FDI attack at the process bus of a DiSt. Moreover, the concept of software defined network in the digital substation has been analyzed in this paper. It is assumed an attacker has access to the process bus of a DiSt. Besides, this substation counts with a SDN switch as shown in Fig. 2. The SDN architecture allows the substation operator to use an intrusion detection protection system (IDPS). The IDPS is in this case centralized and with an SDN controller take actions to remove the attacks when they have been detected. Fig. 3 shows the configuration of the substation grid, the protection IED, MUs and the remaining AC grid. First part of experiments presents the impact of a FDI attack over SVs in the process bus of the DiSt. Besides, it is shown the IDPS behaviour for removing this type of attack. Second part demonstrates the IDPS behavior for a FDI atack on GOOSE protocol.

A. Attack on SVs of the digital substation

The scenario uses the IED's undervoltage function to see the impact of FDI-replay attack. At the first stage recognition and scanning steps were performed. Hence, SVs have been manipulated and reproduced to generate wrong operation of the IED used as subscriber. The SVs traffic has been manipulated and duplicated with a script based on SCAPY [12], this tool facilitates the task of finding vulnerabilities in the DiSt. The attack specifically duplicates one SV packet every 500 ms. The experimental results are presented in Fig. 4. Fig. 4 top shows the SVs voltage streamed at the MU 3 of the busbar

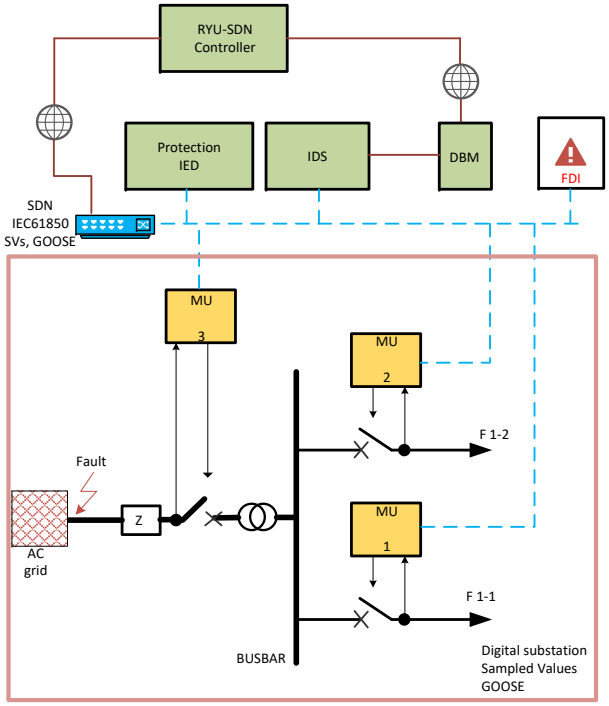

Fig. 3. Digital substation, protection IED and MUs for the experimental results.

and the duplicated SVs. Fig. 4 middle shows the undervoltage trip signal (UVtrip) of the function 27 in the IED and the status of the subscription of SVs in the IED (SVstatus). UVtrip = 0 defines the trip message without activation and UVtrip = 1 represents the activation of the undervoltage trip. SVstatus = 1 represents the correct IED's subscription to the SVs of MU 3. Therefore, SVstatus = 0 defines the subscription is interrupted. The process of duplicating SVs in the process bus produces involuntary changes of status for the subscription by part of the IED. Different activation and deactivation SVstatus are shown in Fig. 4 middle. Before and after the FDI attack SVstatus is 1. However, during the FDI attack the IED losses the correct subscription to the MU's SV.

Additionally, Fig. 4 bottom shows the sample count (smptCnt) attribute of SVs from MU 3 with FDI. The FDI starting and ending times are described in Fig. 4. The first SV is duplicated at 7.1 s and the FDI attack is finished at 13.8 s. Fig. 4 bottom shows the duplicated SVs as spikes of the sample counter attribute. Hence, it is possible to see the changes of SVstatus from 1 to 0 every time the duplicated sampled value is injected i.e. comparing the smpCount signal with spikes and the SVstatus behavior. Thus, the changes are produced some ms after the duplicated SV packet appears.

In addition, the FDI produces an irregular behavior of the IED's UVtrip once the fault is active. It is shown an undesired change from active to deactivation of the UVtrip. The severity of the attack shows that it could lead to a wrong substation control and operation. The system could assume that the fault has been cleared when it is not true. Hence, this could produce a re-closing of the breakers under a fake safe status and it could lead in a severe cascade effect.

It has been shown above the severity and catastrophic effects of a simple replay attack in the DiSt. Fig. 5 shows the behaviour of the IDPS used for the detection of the attacker's SV. Therefore, this IDS detects the attack at 5.3 s, writes and sends a report to a database located at the DBM at DiSt or system operator's control center. The report presents the destination mac address of the SVs under attack, source switch and main destination ports where the SVs are consumed. For the next step another system runs DBM to report an alarm and the blocked ports and highlights the allowed path of the SVs packet. The cleaning flow action has been delayed 5 s in order to visualize the attack during a range of time. Finally, after 5 s of the first attack packet the SDN controller gets an alarm of the attack and reads the report for blocking the source of malicious SV packets for taking the necessary correction actions.

Table I shows the main flows used in the SDN switch before the SVs attack i.e. normal traffic and after the SDN controller sends the correction flow for removing the attacker. For the sake of brevity it is presented the general flows for multicast packets and only the port of the attacker i.e. port 8. Hence, SVs protocol 0x88ba has been flooded in the switch to allow the multiple protection functions of the substation to subscribe directly. Besides, the GOOSE protocol has been dropped in the switch to simplify the presentation of attack on SVs. Once the attack has been detected the cleaning action drops the packets with their respective MAC = MAC_{SV} in Table I, input port (in_port) at the switch and protocol type (dl_type). Additionally, the priority for normal traffic has been set to 10 and a priority = 11 is added for the IDPS action. Therefore, the IDPS flow action is more relevant at the SDN switch.

TABLE I
FLOWS OF THE SDN SWITCH DURING NORMAL TRAFFIC AND FOR CLEANING THE ATTACK OF SVS.

Time range	Priority	Match	Output
Normal traffic	10	dl_type = 0x88ba	FLOOD
Normal Traffic	10	dl_type = 0x88b8	drop
Cleaned attack	11	$in\_port = 8$ $dl\_dst = MAC_{SV}$ $dl\_type =$ 0x88ba	drop

TABLE II
FLOWS OF THE SDN SWITCH DURING NORMAL TRAFFIC AND FOR CLEANING THE ATTACK OF GOOSE MESSAGES.

Time range	Priority	Match	Output
Normal traffic	10	dl_type = 0x88b8	FLOOD
Normal Traffic	10	dl_type = 0x88ba	drop
Cleaned attack	11	$in\_port = 8$ $dl\_dst = MAC_{GOOSE}$ $dl\_type =$ 0x88b8	drop

B. Attack on GOOSE of the digital substation

Figure 6 shows the validation of IDPS for attack on GOOSE messages. This scenario shows how the IDPS allows only one malicious GOOSE packet during the attack and cleaning time ranges. The attack packet appears at 27 s and it is detected and removed by the IDPS, DBM and SDN controller, respectively. Table II shows the main flows used in the SDN switch before the GOOSE attack i.e. normal traffic and after the SDN controller sends the correction flow for removing the attacker. Again this subsection presents only the main flows for IEC 61850 standard. Attacker is connected at port 8 of the SDN switch. GOOSE protocol 0x88b8 is flooded in the switch. SV protocol 0x88ba has been dropped to simplify the presentation of the attack. Once the attack is detected for MAC = MAC_{GOOSE}, the IDPS systems blocks the flow for MAC_{GOOSE} at port 8 in the SDN switch. Normal traffic has priority 10 and the actions of the IDPS have priority 11.

VI. CONCLUSIONS

Approaches like IDPS that keeps safe the power system operation are critical solutions. Hence, its previous analysis and experimentation in a testbed CPS is essential. It has been validated an online IDPS in a testbed cyber-physical system. It is shown how SDN architectures cooperate with the normal operation of the DiSt and keeps the safe operation of DiSt.

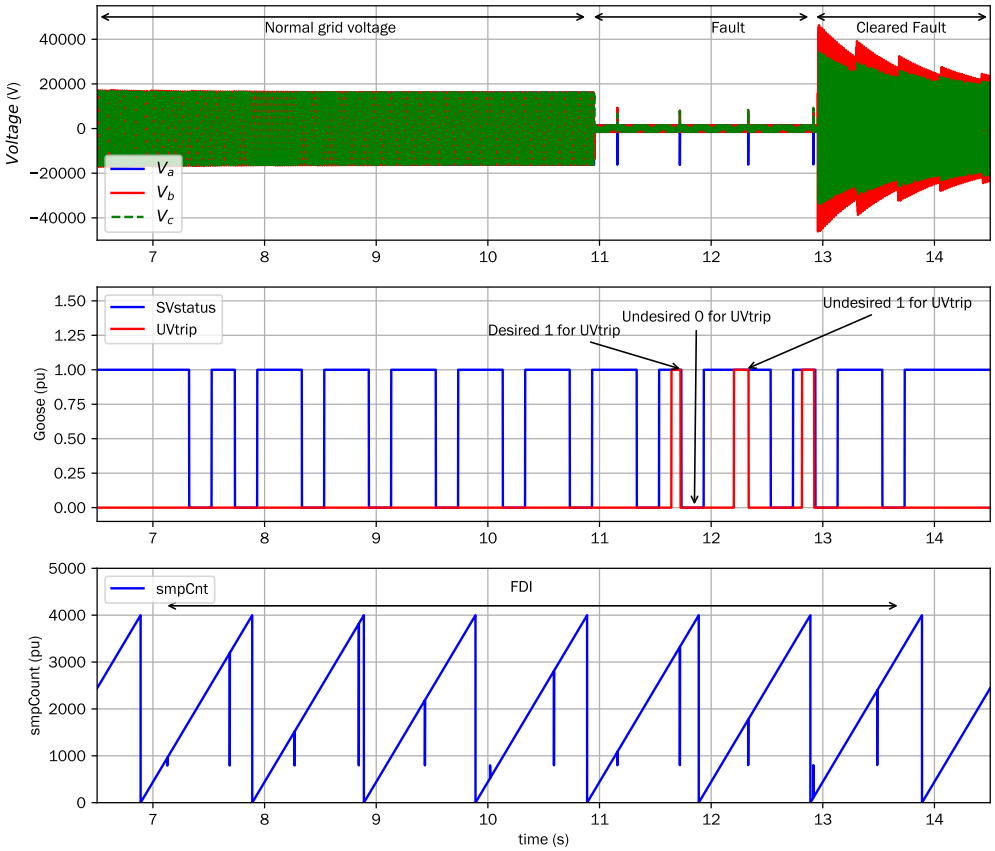

Fig. 4. Results for a FDI at the process bus of a DiSt. Sampled values (top), GOOSE messages (middle) and sample-count attribute (bottom).

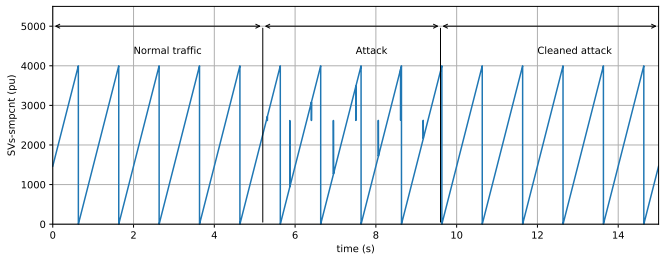

Fig. 5. SV counter behaviour under normal traffic, attack and cleaning by IDPS.

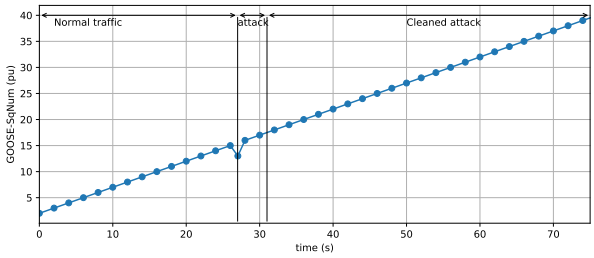

Fig. 6. GOOSE sequence behaviour under normal traffic, attack and cleaning by IDPS.

References

[1] P. Crossley, L. Yang, A. Wen, R. Chatfield, M. Redfern, and X. Sun, "Design and performance evaluation for a protection system utilising iec 61850-9-2 process bus," in *2011 International Conference on Advanced Power System Automation and Protection*, vol. 1, 2011, pp. 534–538.

[2] S. Kumar, N. Das, and S. Islam, "Performance evaluation of a process bus architecture in a zone substation based on iec 61850-9-2," in *2015 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, 2015, pp. 1–5.

[3] S. Kumar, N. Das, J. Muigai, and S. Islam, "Performance evaluation of data transmission in a single and double bus network within the utility substation based on iec 61850," in *2014 IEEE PES General Meeting — Conference Exposition*, 2014, pp. 1–5.

[4] T. Arnold, A. C. Adewole, and R. Tzoneva, "Performance testing and assessment of multi-vendor protection schemes using proprietary protocols and the iec 61850 standard," in *2015 International Conference on the Industrial and Commercial Use of Energy (ICUE)*, 2015, pp. 284–290.

[5] S. E. Quincozes, C. Albuquerque, D. Passos, and D. Mossé, "A survey on intrusion detection and prevention systems in digital substations," *Computer Networks*, vol. 184, p. 107679, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128620312895

[6] S. Sanchez-Acevedo and S. D'Arco, "Towards a versatile cyber physical power system testbed: Design and operation experience," in *2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, 2021, pp. 1–6.

[7] Y. Tang, Qian Chen, Mengya Li, Q. Wang, M. Ni, and XiangYun Fu, "Challenge and evolution of cyber attacks in cyber physical power system," in *2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, 2016, pp. 857–862.

[8] C. Peng, H. Sun, M. Yang, and Y. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1554–1569, 2019.

[9] J. Hong, C.-C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," in *ISGT 2014*, 2014, pp. 1–5.

[10] E. W. Gordon Clarke, Deon Reynders, *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*. Elsevier, 2004.

[11] M. Zillgith, "libiec61850 open source libraries for iec 61850," 2022. [Online]. Available: https://libiec61850.com

[12] R. R. S, R. R, M. Moharir, and S. G, "Scapy- a powerful interactive packet manipulation program," in *2018 International Conference on Networking, Embedded and Wireless Systems (ICNEWS)*, 2018, pp. 1–5.