Towards a Versatile Cyber Physical Power System Testbed: Design and Operation Experience

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

***Abstract*—The present trends in the area of smartgrids indicate that future transmission and distribution systems will heavily rely on digital and on communication technologies to operate. Indeed, the power systems are evolving progressively towards what is denoted as a cyber-physical system. This transition challenges the classical approaches for experimental testing and requires the development of testing platforms for cyber-physical systems able to capture the interactions between physical components, control and monitoring software and the communication infrastructure. This paper presents general considerations and requirements for a cyber-physical testing platform for power systems. The paper provides also examples of a testing platform specifying the characteristics of the major components and a summary of the experience matured in its setup and configuration. Finally, an example of an experiment on a notional smartgrid and the related results are reported.**

***Index Terms*—Smartgrids, Laboratory infrastructure, cyber-physical systems.**

I. Introduction

Power systems are experiencing a rapid technological transition both at transmission and at distribution level to cope with the requirements imposed by the modern society. A first trend is associated to a growing integration of renewable energy sources and to increased relevance to distributed generation including from smaller actors. Furthermore, the continuous improvements in computational capacity and in the capabilities of transferring and processing large volumes of data offer new possibilities for control and automation of power systems at a reasonable cost. Thus, power systems are evolving according to the concept of smartgrids into what are denoted as cyber-physical power systems (CPPS). The dependency on information and communication technology (ICT) and the advances on automation systems for power systems are the drivers for the cyber-physical power system paradigm [1], [2]. A CPPS can be defined as a set of components that integrates the power system, the communication and decision-making technologies using software and physical elements that control the energy exchange and data traffic [2], [3].

The power system is a critical infrastructure and is expected to operate reliably and without interruptions. Thus, any new technology and solution should be extensively tested and validated before being adopted at commercial scale. However, the technological transition of the power systems is challenging the classical approaches for experimental testing and the capabilities of existing testing platforms. Indeed, a general tendency in the past has been to decouple the phenomena associated to the physical systems and on the ICT domain and to test these systems separately or with a strong focus on one of the two and a very simplified representation of the other. These assumptions are less valid in the context of smartgrids and future power systems. This corresponds to a need from utilities, transmission system operators and researchers of developing testing platforms for cyber-physical systems able to capture the interactions between physical components, control and monitoring software and the communication infrastructure [3]. Thus, it is necessary to develop testbeds that allow verification of power system operation while considering the performance of a realistic communication and physical infrastructure [4].

This paper presents general considerations and requirements for a cyber-physical testing platform for power systems in section II. Section III provides also an example of a testing platform in Norwegian National Smartgrid Laboratory in Trondheim specifying the characteristics of the major components and a summary of the experience matured in its setup and configuration. The general objective for the setup is to develop a flexible cyber-physical power system testbed that can be used for multiple tasks. It is envisioned that the user can develop different tests e.g. a test for wide area monitoring and control or a test for coordination of protections in digital substations. Besides it is feasible to test cyber-attacks on the testbed. Hence, validation of cyber security experiments require a communication infrastructure with multiple IT devices. Therefore, section IV describes basic concepts on protocols and cyber-physical threats. A set of possible cyber-physical power systems is described in section V. Finally, examples of an experiment on a notional smartgrid and the related results are reported.

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.

978-1-6654-4875-8/21/$31.00 ©2021 IEEE

This is the accepted version of an article published in 2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)
https://doi.org/10.1109/ISGTEurope52324.2021.9640082

II. Components for a cyber-physical testing platform for electrical systems

The smart grid model can be represented with multiple layers. Thus, in a similar way the CPPS model of the smart grid is composed by components, communication, information and function layers. Therefore, an experimental prototyping of a CPPS will require to integrate and link elements that belong to each different layer. Previous works on CPPS testbeds are focused on hardware-in-the-loop (HiL) validation where a real-time simulator is used to integrate the power system with communication switches or include protection devices such as intelligent electronic Devices (IEDs) [4], [5]. HiL topology of a CPPS is described in [6] with a simulation part and a physical programmable logic controller device. A HiL testbed for energy management systems (EMS) validation with custom software for application of IEC 61850 is demonstrated in [7] while a HiL testbed for protection of transmission power system lines is shown in [8]. Authors in [9] present a testbed for analysis of cyber security for synchrophasor packets based on C37.118. Similar work is presented in [10] for the Texas power system and using a real-time automatic controller.

The survey in [3] presents the testbeds categorized according to the year of publication, target research area, the covered smartgrid domain and the platform type. The 46% of the platforms in the list target cyber-security and 29% are intended for wide-area situation awareness as research areas. From the survey in [3], 25% of the platforms are based on offline simulation only, 35% are hardware based, 29% are based on a real-time simulator and 11% are hybrid. Besides, the authors highlighted that few of the testbeds provide extensive capability to support all research areas. Most of the setups lack complete hardware/software support for all research area applications at the same time.

Recent works target cyber-microgrids as a research area in CPPS. In [5] a software defined network (SDN) is used for describing the challenges for transforming traditional microgrids into networked microgrids (NMs). However, the experiments in [5] are based on a HiL platform. Authors in [11] present a protection technique for NMs based on SDN. A detection of bot attacks on voltage source converter controllers was described in [11]. The method uses the SDN capabilities to authenticate the hosts for data communication. Additionally, the validation platform is of a simulator type and it uses the Mininet with a Ryu controller for the SDN and Matlab/Simulink for the model of NM. The traffic of the packets are based on User Datagram Protocol (UDP) through Mininet. Authors in [4] presented a testbed for cyber-physical power system resilience. The testbed uses a digital real-time simulator (DRTS), a real-time automation controller, protection devices, SDN switch and security solutions in the cloud. Although, the testbed is very flexible; it lacks hardware connection to validate with physical components as the DRTS is used for only power system simulation and link the protection devices. This section lists the components necessary for developing a CPPS platform.

A. Physical hardware components layer

The aim for a CPPS testbed is to mimic a full power system for multiple layers, domains and zones as the configuration shown in Fig. 1 for component, communication and decision layers.

The physical components layer requires the generation systems, transmission, distribution, distributed energy resources (DERs) equipment and customer level premises. It is expected that a versatile testbed will include as many components as possible from the components layer. A possible list of elements for generation are prime movers with asynchronous motor, a power electronics driver and a synchronous generator. For example, the list above can be used to represent a generation plant for hydro-power or thermal generation. Besides, the testbed for CPPS requires communication and decision layers.

B. Real-time simulation

At laboratory scale it can be difficult to reproduce a mechanical prime-mover. Thus, some of the dynamics of a turbine are usually represented with simulation. For transmission it is important to emulate or evaluate system equipment related with the protection or dynamic performance of a transmission system. For this purpose digital real-time simulators are employed when large scale dynamics are necessary on the evaluation of power flows. DRTS and phasor measurement units (PMUs) can be used for wide area control and protection. On the other hand IEDs and DRTS are used at transmission level for protection analysis of transmission systems. Besides, the DRTS, components like power electronic converters are used to integrate and validate integration of renewable energies and high voltage dc transmission. The task of scaling a component of the physical layer sometimes is difficult. Hence, laboratories use real-time simulators for simulating characteristics of power system elements. A digital real-time simulator is a powerful tool for dynamic model emulation and fast control deployment.

C. Communication layer

The communication networks uses ICT devices to provide the physical flow of data from one source to the destination. The devices are mainly IEDs, remote terminal units (RTUs), merging units (MUs), switches and gateways that gather the packets and provides the paths for the data. Besides, the coordination of the CPPS packets are achieved by application of protocols like C37.118, IEC 60870-5-104 (IEC104), Distributed Network Protocol 3 (DNP3), Modbus, and the standard IEC 61850.

D. Software components

Software tools used for simulation of power systems, cyber systems and co-simulation are listed in Paper [1]. However, development of a CPPS testbed requires tools that can be integrated with real power system equipment, DRTSs and ICT devices. Therefore, this paper list some remarkable tools that fulfil that purpose:

This is the accepted version of an article published in 2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)
https://doi.org/10.1109/ISGTEurope52324.2021.9640082

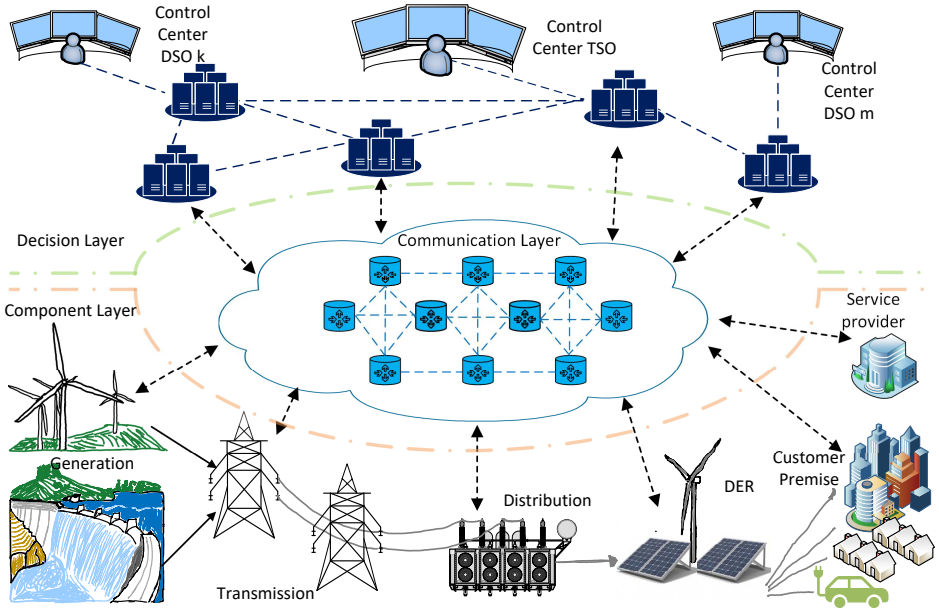

Fig. 1. Layers of cyber-physical power systems.

a) Power systems simulation tools: Due to the capacity to implement the power system models on a DRTS device that enables the interaction with external components some of the simulation tools are: Matlab/Simulink Simpowersym, OPAL-RT-Hypersim, OPAL-RT-ePHASORSIM, RTDS or DigSILENT powerfactory, Power System Simulator for Engineering (PSS/E).

b) Cyber system simulation tool: Mininet, Objective Modular Network Testbed in C++ (OMNet++) and OPNET are tools used on the simulation of networks and control packet flows.

c) Complementary software: Other tools like supervisory control and data acquisition (SCADA) software e.g. from SIEMENS or citect-SCADA are necessary to complement the development of a versatile CPPS testbed and with the purpose of representing the decision layer. Configuration software from ICT devices is usually sold separately. It is necessary to purchase software for configuration of RTUs, IEDs and MUs. Besides, software for monitoring traffic of packets in the communication network is necessary e.g. Wireshark.

III. Description of an Example of a Cyber-Physical Testing Platform

This section describes the cyber-physical testing platform at the Norwegian National Smart Grids Laboratory as an example of an experimental facility including the features reported in the previous section. The laboratory facility is located in Trondheim and jointly operated by SINTEF and NTNU. The cyber-physical laboratory testbed has been designed and incrementally upgraded with the aim of offering easy reconfigurability and a large degree of flexibility in order to serve a wide range of user needs. Fig. 2 shows an illustration of the platform architecture with focus on the interconnection between the components. The hardware IEDs are commercial equipment that use standard industrial protocols to communicate between each other. Hence, it is possible to have field devices used in digital substations automation and obtain SCADA. Besides, this platform can be used for generation, transmission and distribution application functions e.g. the SCADA automatic generation control (SCADA-AGC), energy management systems (SCADA-EMS) or distribution management systems (SCADA-DMS). Thus, protocols are differentiated in the figure with colour labels. The representation of the physical system is hybrid and can include physical hardware components (e.g. power electronics converters, transformer, loads) and emulated power systems following the Power Hardware in the Loop approach. The laboratory features a power amplifier that act as interface between the laboratory bus bars and the real-time simulator and as such can be used to link physical power system devices up to 200 kVA.

The laboratory setup is re-configurable, different levels of process-station buses and wide area traffic can be experienced in a controlled environment. Furthermore, it includes multi-vendor components and it can be used to validate the interoperability of the IEC 61850 standard, the communication with IEC104 or wide area monitoring and control with C37.118 for PMUs. An overview of this setup is shown in Fig. 2 and consists of:

a) Real-time simulator: An OPAL-RT simulator is used for developing the electric power grids and specialized controllers and monitoring of physical devices. Besides, the OPAL-RT includes licenses for use communication protocols such as IEC 61850, IEC104, DNP3, Open Platforms Communications Unified Architecture (OPC UA), C37.118. This allows the simulator to interact at all levels of the SCADA

This is the accepted version of an article published in 2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)
https://doi.org/10.1109/ISGTEurope52324.2021.9640082

architecture and station buses.

b) Power amplifier: The laboratory counts on a 200 kVA power amplifier used for reproducing voltage and currents simulated in the OPAL-RT unit. This amplifier makes possible the interaction of physical devices with simulated power systems.

c) Instrumentation transformers: The testbed uses current and voltage transformers to link the physical signals with the merging units used in a substation level.

d) Intelligent electronic devices: A set of IEDs from multiple-vendors is available in the facility including a protection unit (OC-IED) SIEMENS 7SJ85 for feeder and overcurrent protection plus other functions. The testbed also features a transformer protection unit ABB RET670 (ABB-IED). Both IEDs can be used for PMUs functions.

e) Merging units: Two merging units are used in the testbed. One SEL-401 (SEL-MU) with protection and PMU functions and one 6MU85 (SIE-MU) with protection, PMU functions and can be used as a current, voltage protection function.

f) Grandmaster clock: A SEL-2488 is used as the master clock of the system with precision time protocol (PTP) and IRIG-B ports.

g) Switches: The testbed counts six communication switches with different functions, two industrial switches Planet IGS-6325-16P4S having ports with transparent clock functions, one Aruba 3810M switch (SDN switch), two process bus switches MOXA-PT-7728 with PTP transparent clock function and one HP OfficeConnect 1420 switch.

h) SCADA software: The setup is equipped with AVEVA Vijeo citect as a commercial SCADA development software. The use of this software provides an industrial environment for the SCADA control and monitoring. Additionally, the SCADA includes drivers for IEC104, OPC UA and IEC 61850 client/server.

i) Phasor data concentrator (PDC): A SEL-5073 PDC is used to collect and send the phasors from the PMUs in the network.

j) Configuration personal computer (PC): A Windows 10 PC is used connected to the network for configuring the different IEDs and MUs. Besides, this PC has Wireshark software installed that allows monitoring of the packets in the network.

k) Server computer: A Linux operating system server with 8 ports captures and process the generic object oriented substation event (GOOSE), sampled values (SVs) or PMUs packets in the network. The server can be used for simulating communication networks with a virtual machine mininet. Besides, the server can be used for mirroring ports of the SDN switch or deploying the SDN controller. Additionally, the server can be used to configure the remaining switches. Finally, the server computer is used for developing network applications based on C or python scripts to capture and process traffic.

l) Power electronic converters: The physical power system offers three 60 kVA modular multilevel converters (MMC) and three 60 kVA two-level voltage source converters (2L-VSC). The converters are used together with the power amplifier to develop power-HiL (PHiL) tests.

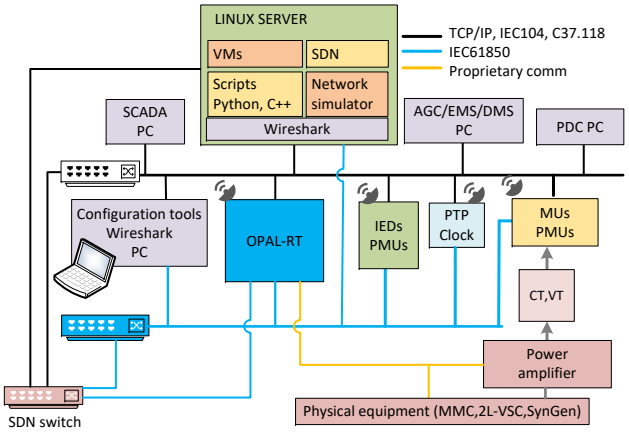

Fig. 2. Overview of the testbed for cyber-physical power systems at the Norwegian National Smart-Grid laboratory.

Fig. 2 gives an idea of the communication flow of the devices: IEC 61850 standard (blue lines), a proprietary protocol for communication between the power amplifier and the real-time simulator (yellow line), and the the transmission control protocol (TCP) - internet protocol (IP), IEC104 and C37.118 (black lines). Additionally, a view of the laboratory testbed is shown in Fig. 3. The equipment listed above is highlighted with the letters.

IV. Communications for Power Systems and Cyber-Security

This section presents basic concepts of the relevant standards and protocols used in the cyber-physical testbed described in this paper. Additionally, the section describes possible cyber-physical threats that can be reproduced within the setup.

A. Communication standards and protocols

The cyber-physical testbed uses IEC 61850 standard in the process bus with traffic packets composed by sampled values, GOOSE messages and PTP. IEC104 or DNP3 can be used for communication from substation to SCADA software. In case the tests performed requires PMUs the C37.118 is used for the wide area network (WAN). Additionally, OPC-UA is used for communication of SCADA and the control center smart-grid functionalities e.g. energy management system.

B. Cyber-physical threats

In a CPPS communication, control and computation technologies is 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 [12] 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

This is the accepted version of an article published in 2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)
https://doi.org/10.1109/ISGTEurope52324.2021.9640082

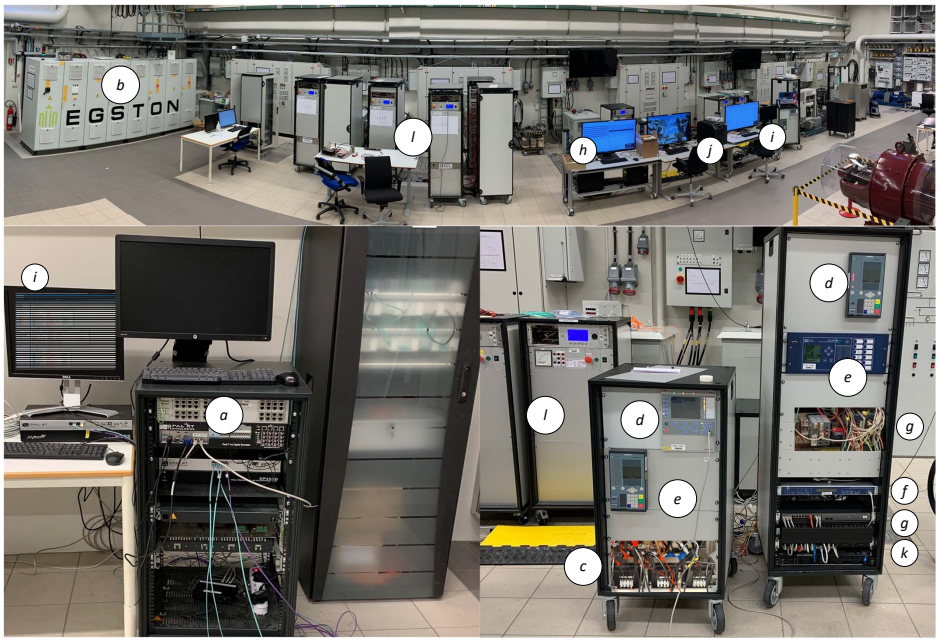

Fig. 3. Overview of the equipment for cyber-physical power systems at the Norwegian National Smart-Grid laboratory. Equipment: (a) Real-time simulator, (b) power amplifier, (c) instrumentation transformers, (d) IEDs, (e) MUs, (f) grandmaster clock, (g) switches, (h) SCADA, (i) PDC, (j) configuration PCs, (k) server computer and (l) power electronic converters.

of communication and control systems in an unpermitted situation, and exploiting security loopholes and defects of communication network'.

The test-bed is equipped with state-of-the-art technology that can be used for testing cyber-security vulnerabilities of the configurations. Some examples of attacks are defined in [12], [13]. Multiple cyber-attacks that can be performed in the test-bed are:

a) Denial of Service (DoS): It is possible to add large amount of useless traffic in the setup to represent a DoS attack. The attack can be performed on the communications network of a substation or a communication channel from the substation to the control center.

b) Bad data injection: the attacker can get access to the monitoring equipment of a transmission or distribution feeder and overwrite values which could lead to wrong operation of the power grid elements such as switches or breaker or reactive power compensators.

c) False data injection (FDI): The attack can target the distribution power system control logic, SCADA, energy management system or communications structure to change important variables.

d) Confidentiality: The attacker can violate the privacy of user or system operator information. At the same time the attacker use the data to reduce performance of the distributed generation units in distribution power systems or generation units in transmission power systems.

V. Examples of Testing Configurations for the Experimental Platform

The setup can be used for Power Hardware in the Loop (PHiL) and HiL tests.

a) PHiL configuration: As an example, a PHiL configuration can be used to test the performance of a MU and an IED of two manufacturers. The real-time simulator reproduces a busbar voltage profile of a simplified substation with a load and the power amplifier reproduces voltage and currents with a physical load. The analog inputs of a MU measures current and voltages and converts them to sampled values (SVs). At the same time the IED subscribes to the SVs of the MU. Finally, Python or C++ scripts executed in the Linux server capture and analyze the interoperability of the system described above. Besides, the human-machine-interfaces of the multiple devices can be visualized in a separate computer that is indicated as the configuration tools device in Fig. 2. Fig. 4 shows a basic network analysis with Wireshark software for the SVs streamed with the MU, the GOOSE messages exchanged and the time synchronization with PTP. The packets/s are presented for the MU's SVs. Clearly there is not packet lost in the network as the SVs line is 4000 packets/s. PTP packets are very constant at the port used with Wireshark. Finally, GOOSE messages vary as function of the different types of messages exchanged between IED and MU and other subscribers like a C++ script.

b) HiL configuration: An example of a HiL test is the validation of a protection function of an IED subscribed to real-time streamed sampled values from the real-time simulator (i.e. the simulator OPAL-RT emulates a MU and replicates voltage and current for fault profiles). This HiL test requires the use of a clock to correctly synchronize the devices.

c) Wide area monitoring protection and control (WAMPAC) configuration: This configuration can be based on the real-time simulation in the OPAL-RT of a wide area

This is the accepted version of an article published in 2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)
https://doi.org/10.1109/ISGTEurope52324.2021.9640082

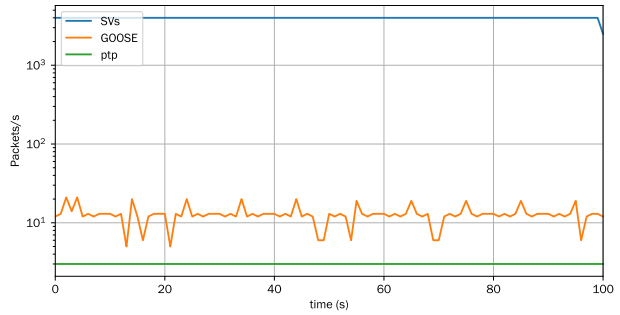

Fig. 4. Wireshark network traffic for the PHiL example.

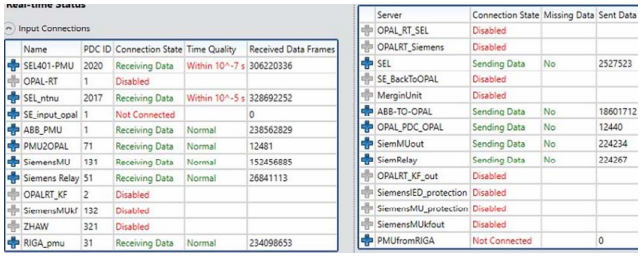

Fig. 5. PDC SEL-5073 configuration for WAMPAC example.

power system. The measured voltages at a bus can be streamed with SVs and IEDs with PMU function can subscribe to the SVs. At the same time the OPAL-RT can stream other PMUs for the remaining buses. Fig. 5 shows the PDC for WAMPAC application. The PDC gathers the phasors from the IEDs acting as PMU and the PMUs from OPAL-RT. The OPAL-RT can be used as a real-time controller to damp low frequency oscillation issues in the wide area power system. Hence, the OPAL-RT subscribes to the PDC and collects the real-time information of the PMUs i.e. the green links at right side of Fig. 5. It is possible to connect a different PC to calculate the output of the low frequency controller. For this example the testbed requires the application of two protocols IEC 61850 and C37.118. Moreover, the testbed can be used in this configuration to attach hardware e.g. a 2L-VSC and analyse the frequency support with wind turbines in the wide area network.

d) SCADA at control center configuration.: The control center of a transmission system operator (TSO) or distribution system operator (DSO) is used to monitor and control the status and position the circuit breakers. The testbed can use the SCADA as the control center providing monitoring and visualization of the physical components. at the same time, OPAL-RT is used to simulate the electrical grid and stream GOOSE messages and SVs to the IEDs. IEDs can be configured to subscribe and publish GOOSE messages with the OPAL-RT. Additionally, the IEDs are used to map signals from the process bus to the station bus with IEC104. Hence, the SCADA control center can communicate to the IEDs in the substation with IEC104 and control or monitor the status of the different circuit breakers.

VI. Conclusions

It has been shown a set of critical elements used for developing a CPPS testbed and the experience of the authors on developing a flexible and versatile CPPS testbed. The current status of the testbed allows the user to choose the degree of complexity of the experiment to be implemented in the laboratory's CPPS. The CPPS testbed presented in this paper can be configure as simulator, HiL or PHiL. Hence, validation of smartgrids technologies are possible under a controlled environment.

The paper shows a set of feasible experiments in the CPPS testbed for behavioral analysis of devices in the process, station or network bus under a cyber attack. Thus, it is demonstrated some of the capabilities of the developed CPPS testbed.

References

[1] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (cpps): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151 019–151 064, 2020.

[2] P. A. Oyewole and D. Jayaweera, "Power system security with cyber-physical power system operation," *IEEE Access*, vol. 8, pp. 179 970–179 982, 2020.

[3] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 446–464, 2017.

[4] M. M. S. Khan, A. Palomino, J. Brugman, J. Giraldo, S. K. Kasera, and M. Parvania, "The cyberphysical power system resilience testbed: Architecture and applications," *Computer*, vol. 53, no. 5, pp. 44–54, 2020.

[5] L. Ren, Y. Qin, Y. Li, P. Zhang, B. Wang, P. B. Luh, S. Han, T. Orekan, and T. Gong, "Enabling resilient distributed power sharing in networked microgrids through software defined networking," *Applied Energy*, vol. 210, pp. 1251–1265, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261917307560

[6] Y. Soupionis and T. Benoist, "Cyber-physical testbed — the impact of cyber attacks and the human factor," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2015, pp. 326–331.

[7] Z. O'Toole, C. Moya, C. Rubin, A. Schnabel, and J. Wang, "A cyber-physical testbed design for the electric power grid," in *2019 North American Power Symposium (NAPS)*, 2019, pp. 1–5.

[8] S. Poudel, Z. Ni, and N. Malla, "Real-time cyber physical system testbed for power system security and control," *International Journal of Electrical Power & Energy Systems*, vol. 90, pp. 124–133, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061516312911

[9] R. Khan, K. McLaughlin, J. H. D. Laverty, H. David, and S. Sezer, "Demonstrating cyber-physical attacks and defense for synchrophasor technology in smart grid," in *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, 2018, pp. 1–10.

[10] H. Huang, C. M. Davis, and K. R. Davis, "Real-time power system simulation with hardware devices through dnp3 in cyber-physical testbed," in *2021 IEEE Texas Power and Energy Conference (TPEC)*, 2021, pp. 1–6.

[11] Y. Li, Y. Qin, P. Zhang, and A. Herzberg, "Sdn-enabled cyber-physical security in networked microgrids," *IEEE Transactions on Sustainable Energy*, vol. 10, no. 3, pp. 1613–1622, 2019.

[12] 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.

[13] 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.

This is the accepted version of an article published in 2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)
https://doi.org/10.1109/ISGTEurope52324.2021.9640082