A Hardware-in-the-Loop SCADA Testbed

Hossein Ghassempour Aghamolki, Zhixin Miao, *Senior Member, IEEE,* Lingling Fan, *Senior Member, IEEE*

***Abstract*—USF Smart Grid Power System Lab (SPS) has developed an hardware-in-loop (HIL) SCADA testbed. This paper describes several communication/control architectures of the testbed with different hardware/software combinations. This testbed will be used to test energy management schemes, power grid cyber attack and mitigation strategies. Phasor Measurement Units (PMUs) synchronized with the common GPS reference signal are used to capture data from a real smart grid system as well as a simulated power network in Opal-RT's real-time simulator. Captured data will be sent to OSIsoft's PI-Server database via different protocols.**

I. Introduction

In this paper, a Supervisory Control and Data Acquisition (SCADA) testbed developed at the SPS lab at University of South Florida will be described. The testbed (shown in Fig. 1) includes several key components: real-time digital simulators to generate data and receive commands, Labview to parse measurements generated by a physical system, OSISoft's PI server to receive, archive data and send out commands. The testbed is Hardware-in-the-Loop (HIL) enabled. The center of the testbed is the PI-system. PI system is a well-known server/software for real-time data management and visualization. The PI system or Plant Information system, delivered by OSIsoft is one of the highly scalable and secure infrastructure for the management of real-time data and events [20]. In PI-system, several software and interfaces are used for receiving data with different protocols and capture all the data in the database.

HIL is a technique for developing and testing of control systems. With HIL simulation, either the control systems or the physical part of a machine or a power system can be replaced by computer models in real-time simulation. In recent research activities, real-time simulators with the capability of HIL has been widely used to facilitate developing laboratory experiments. RTDS and OPAL-RT devices are the most common digital simulator used for such purposes. Real-Time Digital Simulators (RTDS) is used in [3] and [4] to implement and validate over-current, distance, and differential protection schemes.

SCADA systems are used for monitoring and control of power systems. Existing SCADA systems provide non-synchronous data with low density sampling rate (e.g., 1Hz) [5]–[7]. In recent years, research projects focuses on cyber security of conventional SCADA systems rely on SCADA testbeds to test cyber attacks and validate countermeasures. In [8]–[10], SCADA testbeds were developed to assess vulnerabilities introduced by using public access of the communication network. In [11], a SCADA testbed is developed to test and compare designs of integrated information management systems.

H.G. Aghamolki, Z. Miao and L. Fan are with Department of Electrical Engineering at University of South Florida, Tampa, FL 33620 (Email: zmiao@usf.edu).

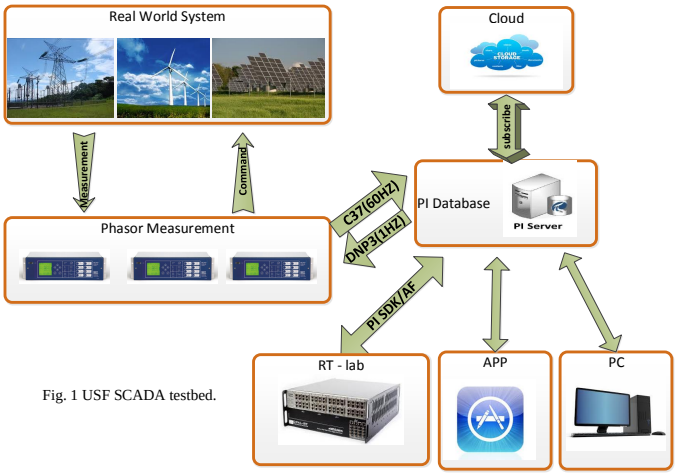


Fig. 1 USF SCADA testbed.

Fig. 1: USF SPS's SCADA testbed.

In this research, a SCADA testbed incorporating PMU data with high sampling rate (60 Hz) is built at USF SPS lab. Traditional SCADA's low rate non-synchronized measurement cannot capture the system dynamics and requires complex nonlinear state estimations [14]. PMUs with GPS common reference signal measures the voltage and current phasors with high-density sampling rate up to 60 Hz. These phasor measurements transmit with the time stamps (synchrophasors), which can help the control system to have an accurate picture of power system and enhance power system situation awareness.

In this paper, we focus on development of a HIL enabled SCADA testbed. This part of research work mainly focuses on real-time simulation, remote monitoring and control of power system operation. The testbed integrates different hardware devices and software packages. Development includes configuring communication interfaces between those devices and packages. Opal-RT real-time digital simulators together with SEL-421 relay/PMU device, LabView boards and OSIsoft's PI-system data center enables the creation of a SCADA testbed. This testbed will be used for validation of comprehensive research on measurements, communication, dynamic modeling, optimization and control of power systems as well as power grid cyber security

The rest of the paper is organized as follows. In Section II, data collecting structures will be presented. Section III presents tools, softwares and communication protocols required for sending the commands and output data to operate the system. Data publishing tools and online applications are presented in Section IV. Section V presents conclusion.

II. Data collecting

This section focuses on different structures used in the testbed for collecting data from different measurement devices. Different protocols and hardware/software combination will be investigated in this section.

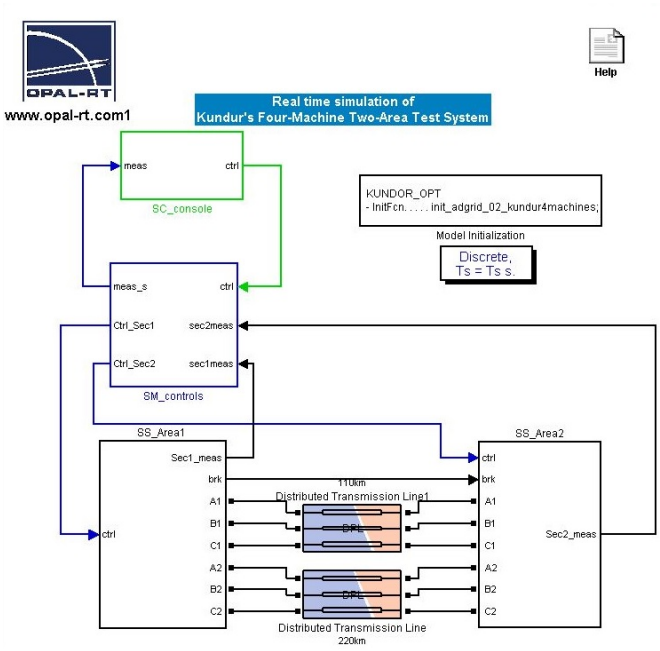


Fig. 2: Kundur's two-area system simulated in RT-Lab software.

A. RT-Lab $\Longrightarrow$ PI Server

Real-time simulation refers to a computer model of a physical system that can execute at the same rate as actual time. Opal-RT real-time simulator is a high performance computer device which can simulate power systems in Matlab/Simulink and send results to industrial displays and Programmable Logic Controllers via digital and analog I/O cards. Digital and analog I/O cards allow the device to send the physical signals to real hardware [18].

As shown in Fig. 2, a desired model of a power system network (Kundur's two area-system) is simulated with Matlab/Simulink software. RT-LAB software will call the Matlab/Simulink to execute the model and convert the separated models into C code for compilation as subsystem simulation on each target processor. Then, the converted model will be downloaded to the specified target (OPAL-RT simulator) by RT-Lab software through the network connection using the TCP protocol. The model will be executed on the target and output signals will be generated by the digital and analog I/O cards. Voltage phasor signals generated by Opal-RT real-time simulator will be sent to IO cards.

Opal-RT simulator's output signals can be directly sent to PI-Server. In this method, real-time simulator will simulate synchronophasor application in parallel with desired power system network simulation and send data with IEEE-C37.118 protocol via internet TCP/IP. In this setup structure, the number of PMUs which can be used for different nodes is limited by the number of network cards install on Opal-RT simulator device. Fig. 3a shows PI-server's collected data from Opal-RT.

B. SEL $\Longrightarrow$ PI Server

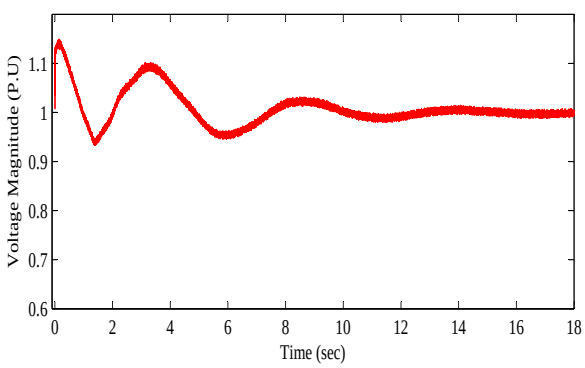
SEL-421 and SEL-351S are protection, automation, and control system devices which can protect transmission line and control two breaker at the same time. These relays are equipped with synchonophasor application, which allows to capture phasor measurements of two different nodes of the system and send the data with DNP3, IEEE-C37.118 and SEL fast message protocols. These devices are able to receive commands with IEC-61850 protocol. With the synchonophasor measurement capability, SEL-421 and SEL-351S are capable of working as a PMU and send the data with sampling rate up to 60 Hz per seconds. They can work as a RTU and send the measured data with DNP3 or SEL Fast Message protocol with the sampling rate of 1 Hz per second [19].

SEL-421 and SEL-351S will be used to measure the output signals. SELs AcSELerator Quickset is a software which can be used for configuring the SEL PMUs and protection relays in order to update CT and VT ratios, selecting synchronophasor data output, defining different protection function such as overcurrent, distance and etc. For synchronophasor measurement applications, SEL-421 have to be provided with GPS common reference signal comes from SEL-2407 Satellite-Synchronized Clock. Time-tagged phasors measured with the 60 Hz sampling rate then will be send through IEEE-C37.118 protocol to the PI-server via internet TCP/IP. IEEE-C37.118 standard defines synchrophasors, frequency, and rate of change of frequency (ROCOF) measurement under all operating conditions. It also specifies methods for evaluating these measurements and requirements for compliance with the standard under both steady-state and dynamic conditions [21]. Since the analog outputs of the simulator are low level voltage and current signals, it is necessary to amplify current and voltage signals to the level acceptable to be fed to the protection relays and PMUs (i.e. 100 V and 1 A). To do so, Voltage and current amplifiers have to be used. Using an amplifier for amplifying the output signals of the simulator to feed into the PMUs is under development at The USF SPS lab.

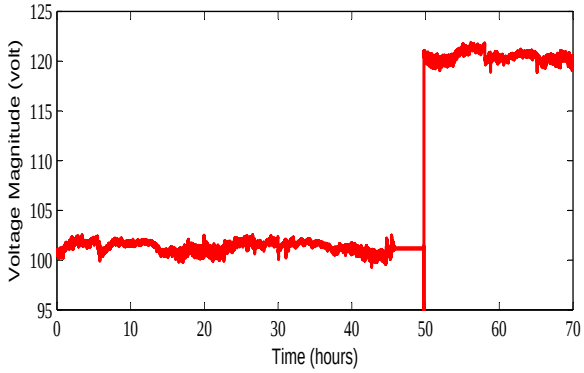
To demonstrate real world data communication using PMU, typical connection of SEL-421 and PI-Server was made in proposed test-bed. In this application, SEL-421 relay measures voltage magnitudes and angles of a three phase AC power supply with 60 Hz sampling rate and sends the data with IEEE-C37.118 protocol to the PI-Server through TCP/IP based Internet connection. Fig. 3b shows real output signals of the AC power source and phasor data collected in PI-Server.

C. Labview $\Longrightarrow$ PI Server

LabVIEW is a graphical programming tool for test, measurement, and automation and is widely used as a virtual instrumentation tool. It allows users to develop sophisticated measurement, test, and control systems using intuitive graphical icons and wires that resemble a flowchart. This tool is

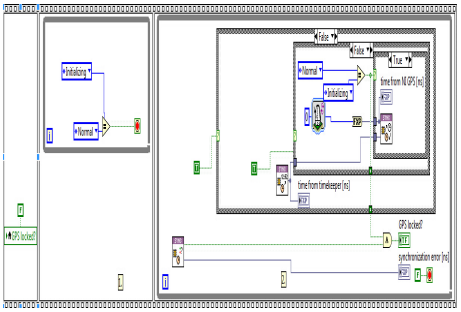


(a) Phase A voltage magnitude of the generator 1 collected from Opal-RT simulator output

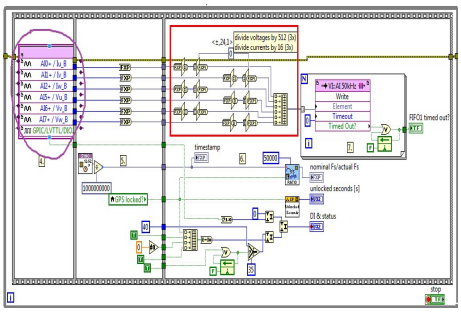


(b) Phase A voltage magnitude output collected from SEL-421

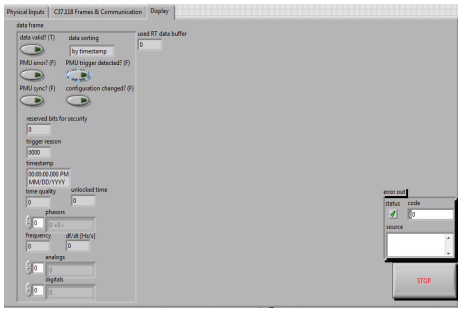
Fig. 3: measurement data collected by PI-server: a. Output data from Kundur's system simulation in Opal-RT simulator. b. Output data from three phase AC voltage source, collected by SEL-421



(a) LabView simulates GPS clock signal



(b) LabView simulates synchronophasor application



(c) LabView's GUI interface will be used to change simulation variables

Fig. 4: LabView simulates synchronophasor application and send the measured data with IEEE-C37.118 protocol.

increasingly being used in development of laboratory test applications. The applications are user friendly and the test output can be checked instantly. In addition, one of the major advantages of LabVIEW, apart from being simple to use, is the ability to work with a number of hardware interfaces using real world analog and digital signals. LabVIEW programs work as simulation or data acquisition applications [7].

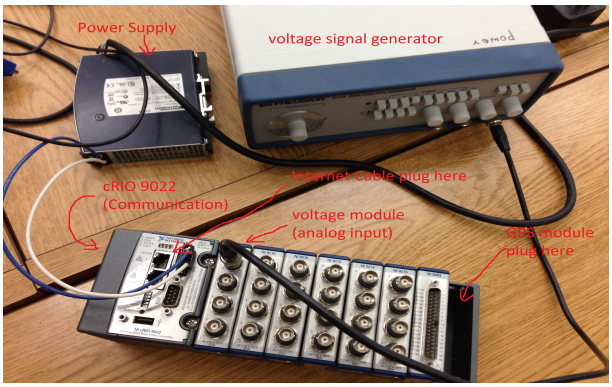


Fig. 5: Architecture of the LabView based test-bed setup.

Fig. 5 Shows the architecture of the LabView based test-bed setup. To demonstrate the test-bed's capabilities, a single-phase voltage source generates the AC voltage. Proposed architecture has National Instrument cRIO-9022 embedded real-time controller. The cRIO-9022 is part of the high-performance CompactRIO programmable automation controller platform. It features an industrial 533 MHz free-scale MPC8347 real-time processor for deterministic, reliable real-time applications and contains 256 MB of DDR2 RAM and 2 GB of nonvolatile storage for holding programs and logging data [22]. The controller is designed for low power consumptions. Therefore, a 9 to 35 volt DC voltage supply can be used as a power source for this controller. In addition, cRIO-9022 provides two Ethernet ports for communication with LabView software and synchronophasor applications. Furthermore, the controller is equipped with NI-9215 and NI-9207 analog voltage and current measurement modules. The voltage is measured by NI-9215 modules and sent to the LabView software through a network connection. For synchronophasor applications, GPS common reference signals have to be provided using NI-9467 timing and synchronization module. For testing purpose, this signal can be provided by a GPS signal simulating block inside LabView software. Currently, the simulation approach is used to provide required GPS signal in existing test-bed.

LabView simulated model consists of three parts: GPS sig-

nal simulation, C37.118 protocol creation, and GUI interface to control the model. Figure 4 shows all three parts of LabView model for synchronophasor application. Basically, the voltage analog input module, measures the voltage with 100 kS/s sample rate in time domain. Therefore, voltage's magnitude and angle are calculated inside LabView model in order to create IEEE-C37.118 protocol messages. Then PMU data with 60 Hz sampling rate is sent to PI-server database through internet connection.

D. Real-world measurements $\Longrightarrow$ PI Server

A new project is started recently at the USF SPS lab to explore the integration of storing solar energy in new battery systems. As part of the project, a 100 kW solar photovoltaic (PV) system has been installed on the top of the USF St. Pete campus's 5th Avenue South parking garage. Energy produced by the new solar PV system is to be stored in the new battery systems. High resolution data will be collected on all aspects of PV and energy storage. Operating strategies will be developed to maximize synergy between the two systems. The new energy storage system will be operated by the USF SPS lab group in conjunction with two existing 20 kW USF storage systems. Furthermore, a central control center will be developed in order to collect the measured data, optimize the PV-Battery system. All those facilities together with communication hardware/software combinations shape a new smart grid test-bed to investigate various algorithms and protocols for smart grid control and measurement systems.

The existing communication system protocol for this project limited to Moudbus protocol. The completed setup architecture of the smart grid test-bed will be different. Fig. 1 shows the proposed architecture of smart grid test-bed system. In this system, SEL-421, SEL-351S Relay/PMU and National Instrument cRIO-9022 controller will be used to read the data from PV/Battry stations in different locations. Since SEL based and LabView based communication test-beds already have been created and tested at the USF SPS lab, implementing proposed smart grid test-bed architecture will be much easier than before for the next step of the smart grid test-bed development. Therefore, parallel to the existing Modbus protocol, captured data will be sent to the PI-server via IEEE-C37.118 protocol as well. In this testbed setup, SEL-421 will be used to collect AC side measurement data, including inverter's outputs, while cRIO-9022 will be used for collecting battery-side DC measurement data. This way, the real-time data can be collected over any period ranging from minutes to days or more, only limited by the amount of space allocated for the data storage.

In the existing approach, Modbus master is collecting all the measured data, including both AC-side and DC-side voltages and powers. Collected data is then sent to the data center with Modbus protocol. In order to collect the data with Modbus protocol, both Moudbus Poll software [23] and PI-server are used. Using PI-server is important since the Modbus Poll software does not have the capability for saving data for a long time. It is more suitable to use Modbus poll software for observing the real-time status of the system and sending necessary online commands for operating the system. Also, Modbus protocol can only provide low rate sampling data (1 Hz). Therefore, developing the proposed test-bed architecture will help to provide researchers with the higher resolution data which is needed for the dynamic studies of the PV-battery systems.

III. Command and data sending structure

In the previous section, we investigated test-bed architecture to receive and save recorded data in PI-Server database. Collected data then will be used as an input to the optimization algorithms to find the best operating point for the system. Optimization results will lead to finding out the appropriate commands and the output power schedule for the system. therefore, those commands have to be sent to either real-time simulator to update reference points of the simulated network or to be sent to PV-Battery controllers for getting the desire power output scheme. Two different protocols can be used for such purposes, DNP3 and Modbus.

A. Modbus protocol for command sending

Modbus is an application layer messaging protocol, positioned at level 7 of the OSI model, which provides client/server communication between devices connected on different types of buses or networks. Modbus is a request/reply protocol and offers services specified by function codes which are elements of Modbus request/reply PDUs [24]. Modbus continues is a popular protocol for millions of automation devices to communicate with serial connections. Network based Modbus protocol is becoming more and more popular in recent years. TCP/IP based DNP3 can be accessed at a reserved system port 502.

Both PI-server and Modbus Poll software can be used for sending commands and data with Modbus. In PI-server, each command is defined as a specific tag (data point). By changing these output tags, appropriate commands will be sent to Modbus master. Also, both single register and multi register writing are supported in PI-server. In Modbus poll we have the same capability to write single or multi registers at the same time. Therefore, for real-time commands sending, there is no big difference between the two software packages. Using PI-server has the advantage of data archive and automatic coding for operation. Fig. 6 shows Modbus Poll environments for sending operation commands to the PV-Battery system located in USF St. Pete campus.

B. DNP3 protocol for command sending

DNP3 is based on the standards of the International Electrotechnical Commission (IEC) Technical Committee 57, Working Group 03. This working group has been working on an OSI 3 layer "Enhanced Performance Architecture" (EPA) protocol standard for tele-control applications. DNP3 the standard and rules for computers and master station computers located in different locations in order to communicate data and control commands. DNP3 is specifically designed for SCADA

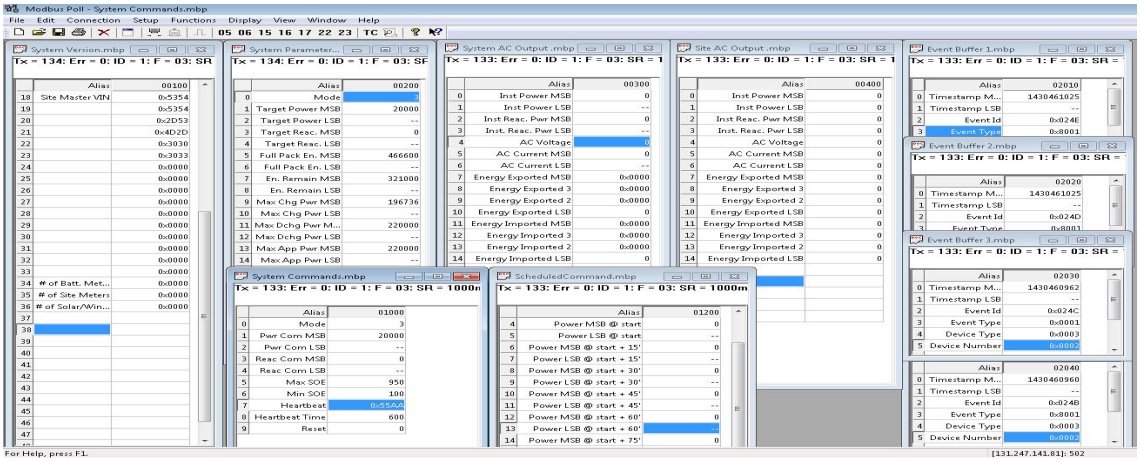


Fig. 6: Modbus Poll software is used to operate PV-Battery system.

(a) PI-processbook **(b)** PI-Coresight **(c)** Excel with PI-datalink

Fig. 7: Pi-client tools is used for accessing PI-server data

applications and was designed to optimize the transmission of data acquisition information and control commands from one computer to another [25]. PI-server DNP3 interface will be used to send the command data for system. In Real-time simulator based test-bed, after optimizing the system based on recorded data, command will be sent to Opal-RT simulator through DNP3 protocol from PI-Server. It will help to change different control reference points for making desired changes in the system topology and working point.

IV. ONLINE APPLICATIONS AND DATA DEMONSTRATION

This section investigates the tools and software for publishing data as well as proposed architecture for online applications. PI client is the most important tools to access the collected data in PI-server. Several PCs are given client access in the SPS lab. A complete PMU farm is built inside PI-server consisting all PMU data collecting from different locations. These PMUs include SEL-421 located in USF engineering building, SEL-421 located at USF Research and Innovation Center, Opal-RT based and RT-Lab based PMU located in USF SPS lab and Modbus master measurement located in USF ST. Pete campus. Each client can access the data with different software and platforms like PI-Processbook, PI-Coresight and excel spread sheet. PI-Coresight is an intuitive, web-client tool that helps users quickly and easily analyze data and it provides secure access to the PI System's data with different access level [26]. PI-Processbook is a software that can efficiently display current and historical data residing in the PI System and other sources. Also, it has the ability to create interactive graphical displays that can be saved and shared with others [27]. PI-DataLink provides a graphical interface to retrieve data and build functions and calculation. Also, datalink functions are embedded in spreadsheet cells and can provide active updates of data from the PI-Server. Combined with the computational, graphic and formatting capabilities of Microsoft Excel, DataLink offers powerful tools for gathering, monitoring, analyzing, and reporting PI Data [28]. Fig. 7 presents different Pi-client tools using in the USF SPS lab.

For online applications, collected data from different locations can be read by either spread sheet datalink commands then feed to Matlab or directly fed to the Matlab workspace with appropriate cedes. In either case, Matlab automatically reads collected data from PI-Server database. C-sharp codes can be used for automatically reading the data from PI-server as well. Currently, we used C-sharp codes to read the data with spread sheet datalink commands and feed the data to Matlab code. Then, desired optimization algorithms optimize the operation of the system and produces appropriate commands to operate the system. Those commands, then will be sent back to the system by using either Modbus or DNP3 communication protocol. At the present time, sending the commands automatically to the system controllers is still under

development process.

V. Conclusion

This paper describes several communication architectures for a SCADA testbed with different hardware/software combinations. This test-bed can be used to test energy management schemes, power grid cyber attack and mitigation strategies. In this testbed, phasor Measurement Units (PMUs) synchronized with GPS reference signals are used to capture data from the real-world smart grid system as well as simulated power network in OPAL-RT simulator. Different architectures/protocols are used in terms of communication. IEEE-C37.118 and Modbus protocols are used to collect the data with PI-Server. The feature of this SCADA testbed is its capability of communicating high resolution data compared to conventional SCADA systems.

References

[1] L. D. Feisel and A. J. Rosa, "The role of the laboratory in undergraduate engineering education," *Journal of Engineering Education*, vol. 94, no. 1, pp. 121–130, 2005.

[2] P. Menghal and A. Laxmi, "Real time control of electrical machine drives: A review," in *Power, Control and Embedded Systems (ICPCES), 2010 International Conference on*, Nov 2010, pp. 1–6.

[3] E. Schweitzer, D. Whitehead, A. Guzman, Y. Gong, M. Donolo, and R. Moxley, "Applied synchrophasor solutions and advanced possibilities," in *Transmission and Distribution Conference and Exposition, 2010 IEEE PES*, April 2010, pp. 1–8.

[4] A. Saran, S. Palla, A. Srivastava, and N. Schulz, "Real time power system simulation using rtds and ni pxi," in *Power Symposium, 2008. NAPS '08. 40th North American*, Sept 2008, pp. 1–6.

[5] P. Kundur, N. J. Balu, and M. G. Lauby, *Power system stability and control*. McGraw-hill New York, 1994, vol. 7.

[6] M. Anjia, Y. Jiaxi, and G. Zhizhong, "Pmu placement and data processing in wams that complements scada," in *Power Engineering Society General Meeting, 2005. IEEE*, June 2005, pp. 780–783 Vol. 1.

[7] R. Reddi and A. Srivastava, "Real time test bed development for power system operation, control and cyber security," in *North American Power Symposium (NAPS), 2010*, Sept 2010, pp. 1–6.

[8] C. Davis, J. Tate, H. Okhravi, C. Grier, T. Overbye, and D. Nicol, "Scada cyber security testbed development," in *Power Symposium, 2006. NAPS 2006. 38th North American*, Sept 2006, pp. 483–488.

[9] C. Queiroz, A. Mahmood, J. Hu, Z. Tari, and X. Yu, "Building a scada security testbed," in *Network and System Security, 2009. NSS '09. Third International Conference on*, Oct 2009, pp. 357–364.

[10] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of scada control systems (tasscs)," in *Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES*, Jan 2011, pp. 1–7.

[11] N. Lu, P. Du, P. Paulson, F. Greitzer, X. Guo, and M. Hadley, "The development of a smart distribution grid testbed for integrated information management systems," in *Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES*, Jan 2011, pp. 1–8.

[12] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *Smart Grid, IEEE Transactions on*, vol. 4, no. 2, pp. 847–855, June 2013.

[13] T. Yardley, R. Berthier, D. Nicol, and W. Sanders, "Smart grid protocol testing through cyber-physical testbeds," in *Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES*, Feb 2013, pp. 1–6.

[14] P. Yang, Z. Tan, A. Wiesel, and A. Nehora, "Power system state estimation using pmus with imperfect synchronization," *Power Systems, IEEE Transactions on*, vol. 28, no. 4, pp. 4162–4172, Nov 2013.

[15] U. Adhikari, T. Morris, N. Dahal, S. Pan, R. King, N. Younan, and V. Madani, "Development of power system test bed for data mining of synchrophasors data, cyber-attack and relay testing in rtds," in *Power and Energy Society General Meeting, 2012 IEEE*, July 2012, pp. 1–7.

[16] L. Vanfrett, "Developing experimental research platforms and pmu data applications for wide area systems," in *[Online] Available: http://idisk.me.com/vanfretti/Public /presentations/2011-LV-Lund-LCCC-Seminar-edited-slides.pdf*, 2011.

[17] L. Vanfretti, M. Chenine, M. S. Almas, R. Leelaruji, L. Angquist, and L. Nordstrom, "Smarts laba laboratory for developing applications for wampac systems," in *Power and Energy Society General Meeting, 2012 IEEE*. IEEE, 2012, pp. 1–8.

[18] "Distributed real-time power system," in *Opal-RT manuals, www.opal-rt.com*, 2012.

[19] I. Manual, "Sel-421 relay, protection and automation system," 2009.

[20] V. Skendzic and A. Guzma, "Enhancing power system automation through the use of real-time ethernet," in *Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources, 2006. PS '06*, March 2006, pp. 480–495.

[21] "Ieee standard for synchrophasors for power systems," *IEEE Std C37.118-2005, (Revision of IEEE Std 1344-1995)*, pp. 1–57, 2006.

[22] N. I. Webpage, "http://www.sine.ni.com," 2015.

[23] modbus tools webpage, "http://www.modbustools.com," 2015.

[24] I. Modbus, "Modbus application protocol specification v1. 1a," *North Grafton, Massachusetts (www. modbus. org/specs. php)*, 2004.

[25] K. Curtis, "A dnp3 protocol primer," *DNP User Group*, pp. 1–8, 2005.

[26] O. webpage, "http://picoresight.osisoft.com," 2015.

[27] ——, "https://www.osisoft.com/software-support/products/pi-processbook.aspx," 2015.

[28] ——, "https://www.osisoft.com/software-support/products/pi-datalink.aspx," 2015.