The Use of System in the Loop, Hardware in the Loop, and Co-modeling of Cyber-Physical Systems in Developing and Evaluating Smart Grid Solutions

M. Kezunovic, A. Esmaeilian
Texas A&M University

G. Manimaran
Iowa State University

A. Mehrizi-Sani
Washington State University

Abstract

This paper deals with two issues: development of some advanced smart grid applications, and implementation of advanced testbeds to evaluate these applications. In each of the development cases, the role of the testbeds is explained and evaluation results are presented. The applications cover the synchrophasor systems, interfacing of microgrids to the main grid, and cybersecurity solutions. The paper hypothesizes that the use of the advanced testbeds is beneficial for the development process since the solution product-to-market cycle may be shortened due to early real-life demonstrations. In addition, solution users' feedback to the testbed demonstration can be incorporated at an early stage when making the changes is not as costly as doing it at more mature development stages.

1. Introduction

In last few decades, smart grid emerged as a solution to fulfill the need to facilitate connection of renewable energy resources to reduce the carbon footprint compared to legacy fossil fuel plants [1]. Smart grid protection, monitoring, and control tasks are improved by adding system-wide monitoring and control capabilities through synchrophasor systems [2]. In addition, smart grid allows interfacing of the legacy grid with microgrids, plug-in hybrid electric vehicles, and energy storage [3]. As a result of such technology deployments, there is a growing concern about cybersecurity and privacy of smart grid solutions [4].

The practical approach to study impacts of such advancements on the power grid is through implementing proper testbeds, so to avoid the demonstrations interfering with actual power systems operation. New generation testbeds are designed and implemented using actual power system control equipment interfaced with actual grid and/or simulation software to allow replication of full-scale cyber-physical system performance at a large laboratory scale. Several papers addressed the development of the power system cyber-physical testbeds [5-17]. In [5-9], concept of end to end testing

using the system in-the-loop (SIL) testbed is presented. In [10-15], hardware-in-the-loop (HIL) testing platforms for different studies including distributed generation and power electronic interfaces are discussed. Examples of cyber-physical testbeds to study different concerns related to power system cyber-attacks can be found in [16, 17]. These papers describe the testbed setup but quite often do not elaborate on the full benefits of large-scale testbed concept.

Our paper describes the following three testbeds and elaborates on their benefits.

The system-in-the loop (SIL) testbed is used to evaluate a new synchrophasor based fault location (FL) application [18]. The full-scale end-to-end synchrophasor testbed allows evaluation of the FL algorithm under real power grid operating conditions, and its robustness can be quantified under various failures in the synchrophasor infrastructure.

A real-time simulation platform for hardware-in-the-loop evaluation of distribution-level microgrid controllers is developed and implemented in [19]. The proposed solution turns an offline power system simulation tool into an online tool by wrapping it with the necessary timekeeping and interface algorithms, which can be used to test the performance of physical controllers.

The Cyber-Physical Security (CPS) testbed is a co-simulation platform that integrates real, simulated, and emulated components or subsystems [20, 21]. It is composed of three key components: (i) industry-grade SCADA, (ii) RTDS, Opal-RT for real-time digital simulation of power system, and (iii) a wide-area communication emulator for mimicking the channel characteristics of communication between substations and control center.

A brief background of each testbed concept is explained in Section 2. In Sections 3, 4, and 5, the procedure to set up the SIL, HIL, and co-simulation testbed Use Cases is outlined, the hypothesis why the testbeds are beneficial and how the benefits can be achieved is stated, and examples of the results of Use Case testing of fault location algorithm, renewable generation interfacing, and cybersecurity solutions are presented. The conclusion with summary of contributions is given in Section 6.

2. Background

The SIL testbed assumes that a control system and a physical system are tied together in an implementation that resembles the production environment of actual control systems. The only differentiation is that the SIL production environment is not connected to control actual power system but a system model instead. An example of an SIL for a synchrophasor testbed is shown in Figure 1.
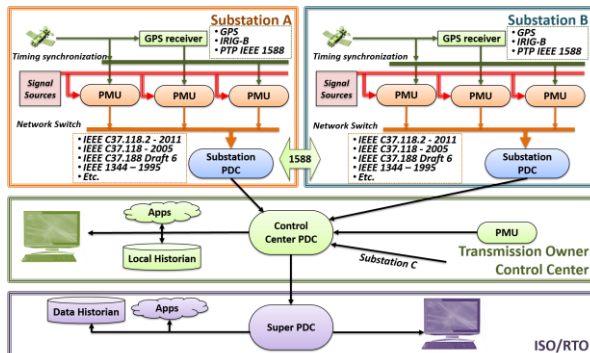

Figure 1. Synchrophasor SIL testbed architecture

This production system is implemented using commercial products and instrumented to allow for new applications to be embedded and evaluated through interaction with the rest of the system components. It consists of multiple Phasor Measurement Units (PMU), substation and control center Phasor Data Concentrator (PDC), and a Software Defined Network (SDN) controller for emulation of different communication protocols and network features. It contains a full suite of synchrophasor software from Alstom/GE, integrated with OSISoft PI historian and Esri GIS software. The input measurements come from three sources: actual network, real time simulator (OPAL-RT), and signal generator. The power system network is modeled after an actual power grid, so the test cases are scaled to a real-life application. As elaborated later on in this paper, this testbed is used to evaluate a new fault location technique developed using measurements of the electromechanical wave propagations initiated by system faults [18].

Figure 2 shows the overall structure of the proposed HIL simulation platform. This platform uses available commercial off-the-shelf components for an accurate and functional solution to evaluate the performance of a physical controller for microgrid applications. This solution has the added advantage of flexibility, affordability, and ease of use. The size of the system, number of I/O (input/output) signals, and the controller hardware can all be customized as needed based on the
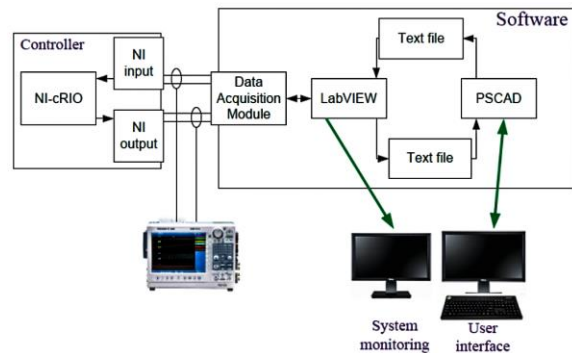

Figure 2. Overall structure of the proposed software-based HIL simulation platform

exact application. As discussed later in this paper, the setup developed in this work uses PSCAD/EMTDC as the simulation engine, NI LabVIEW as the hardware interface, and NI cRIO as the physical controller hardware.

Figure 3 shows the architecture of the PowerCyber testbed that consists of SCADA hardware/software with emulation and simulation capabilities that include substation automation system (Siemens SICAM PAS), control center software (Siemens Power TG), SCADA and substation communication protocols (DNP3, IEC 61850, IEEE C37.118), and security technologies (Scalance: Firewall, VPN), four multifunction protection relays (7SJ610, 7SJ82), three SEL 421 PMUs and a Phasor Data Concentrator (PDC) to provide a realistic electric grid cyber infrastructure. Power system simulations are performed using real-time digital simulators such as RTDS and Opal-RT and using DIgSILIENT PowerFactory software for non-real time analysis.

The testbed employs virtualization technologies to address scalability concerns and reduce development cost. The testbed has also been integrated with the Internet Scale Event and Attack Generation Environment (ISEAGE) [22] to provide wide-area network emulation and advanced attack simulation. The testbed uses cyber-attack tools such as nmap, WireShark, and Nessus for cyber security and attack-defense experimentations. The testbed provides a cyber-physical power grid environment wherein realistic experiments on wide area monitoring, wide area control, wide-area protection (WAMPAC), and distributed decision making in the smart grid can be carried out. The testbed is being utilized for carrying out three main research tasks: (a) vulnerability analysis in the cyber layer; (b) impact analysis due to successful cyber-attacks; and (c) cyber security validations and attack-defense evaluation studies to evaluate the effectiveness of security measures [21].
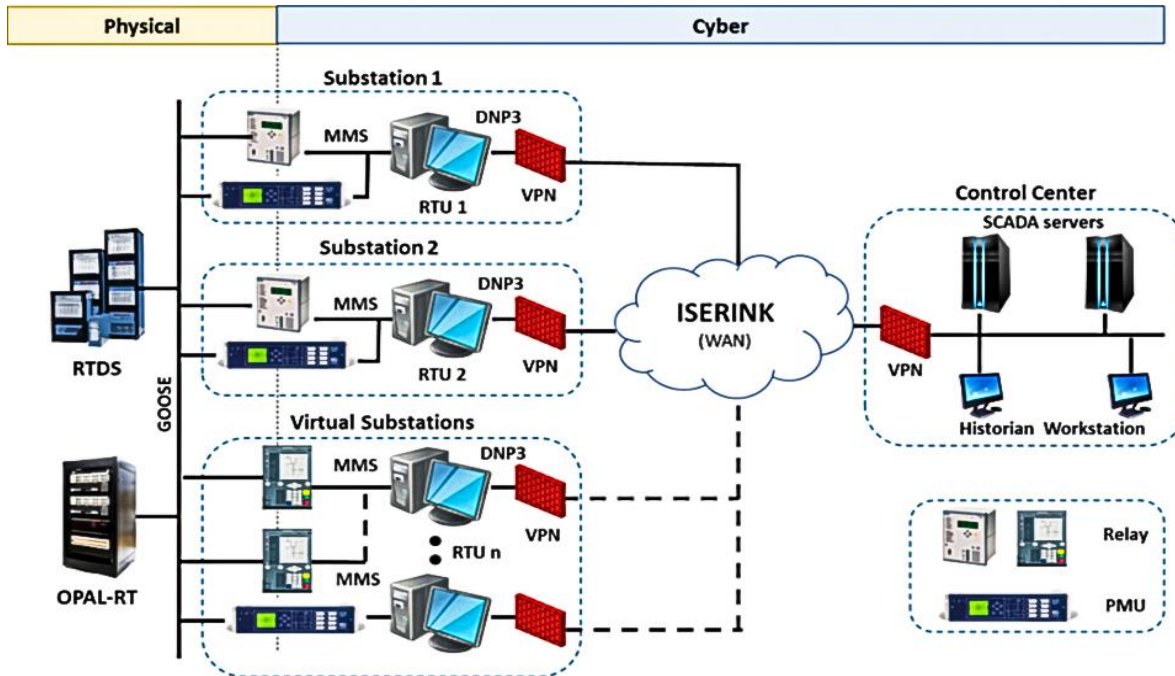
Figure 3. PowerCyber CPS Testbed

3. SIL testbed use for developing and evaluating synchrophasor fault location application

In the last two decades, availability of synchronized measurements utilizing PMU devices has become a turning point in power system monitoring, protection and control [23]. In this section, we use the SIL synchrophasor testbed to evaluate a newly proposed fault location method in realistic field conditions.

3.1. Application development

Faults occur in power system due to reasons including extreme weather condition and vegetation, animal or human contacts. Once protective relays send trip command to circuit breakers to clear the fault, the location of fault must be determined to facilitate troubleshooting and minimize restoration time [24].

Following a fault on a transmission line, powerflow re-routes in the power system, and triggers a mismatch between generators' electrical and mechanical torques which are located in the vicinity of fault. To compensate the mismatch, each generator rotor angle changes with regard to its reference angle which results in powerflow redistribution. Similarly, the adjacent generators' rotor angles start slipping against their reference angle to compensate the mismatch. In this manner, the oscillation known as "electromechanical wave" propagates through the entire network [25].

These electromechanical waves travel through different paths with limited speed (compared to electromagnetic one) and arrive at remote buses with specific time delays, which could be detected by monitoring phasor angle at PMU locations in the system. Since propagation delay depends solely on the network parameters, Dijkstra's shortest path algorithm can be deployed to build a database of propagation delays between different buses of the system. The proposed fault location method detects Time of Arrival (ToA) of electromechanical waves at different PMU locations using first and second derivative of phase angle signal. Then determines the faulty line using an optimization algorithm that minimizes the norm of accumulative error between actual measured delay and calculated error from the database. Once the faulty line is detected, the fault location is calculated within the faulty line using binary search algorithm [19].

To evaluate the performance of such application prior to deployment in the field, one has to represent a complex power system and to take into account various data quality issues in the synchrophasor infrastructure. It allows verifying the performance of application in the conditions very similar to what is found in the field.

3.2. Testbed set up

Figure 4 shows the configuration of the SIL testbed for evaluation of fault location application. The testbed is implemented using various commercial solutions acquired through partnership agreements with major
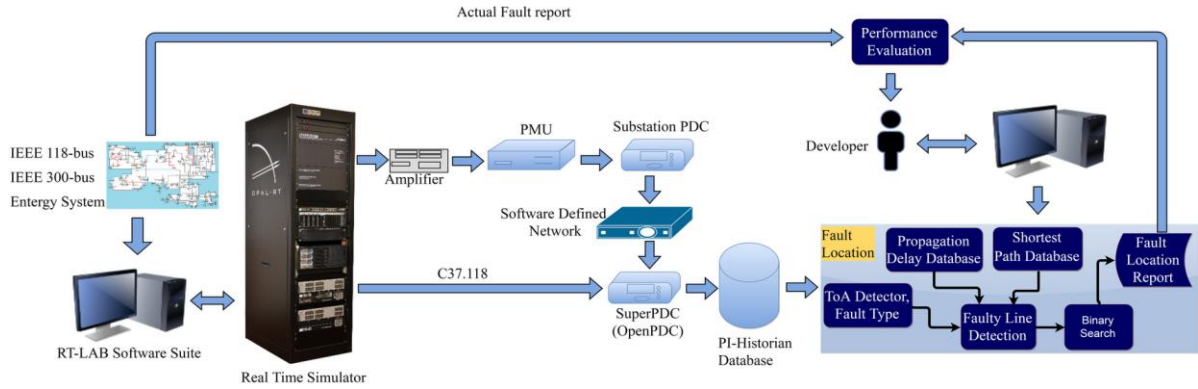
3

Figure 4. SIL testbed configuration for FL evaluation

vendors in this area, such as Opal-RT, OsiSoft and several PMU vendors.

The evaluation using the testbed configuration shown in Figure 4 allows the users to do the following:

- Run real-time simulation of different power system models and studies (such as faults, load or generation outage and topology control) with Opal-RT simulator. The RT-LAB software suite is the connection point between software and hardware parts of the SIL system.
- Send voltage/current signals through Opal-RT analog I/O board and scale them with power amplifiers. RT-LAB software suite allows employing virtual PMUs within software and directly sends PMU streams via C37.118 protocols to PDC.
- Measure phasor (GPS synchronized) values of signals using PMUs from different vendors.
- Collecting phasors from PMUs using substation PDC.
- Transfer substation PDC data to OpenPDC (control center PDC) using SDN, which allows simulation of different communication system failures (such as latency and data loss).
- Archive phasor data using PI-Historian server.
- Perform fault location study on a complex system model which can better reflect actual field conditions. Evaluate performance of fault location application by comparing its output results with the input fault scenarios inserted with SIL simulations.

Figure 5 shows the physical connection of SIL synchrophasor testbed equipment/software setup.
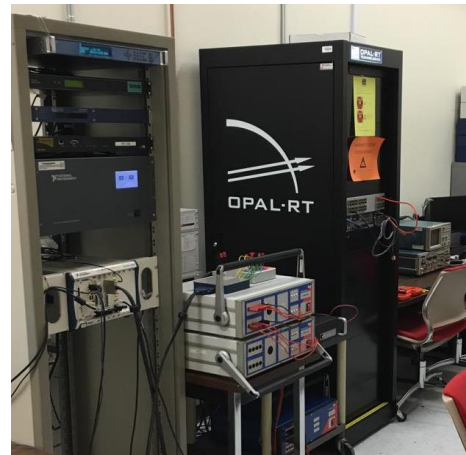
3.3 Use-Case 1: Impact of power system

The fault location application is initially tested using IEEE118 bus test system [19]. The SIL testbed makes it possible to test FL method with various scenarios such as changing fault specifications, size

Figure 5. SIL synchrophasor testbed physical setup

(number of buses, type of lines), and system operating conditions prior to or during fault. The test using actual size system from a utility interested in the implementation is underway.

A summary of results for a few test cases with different fault specifications is listed in Table I. The proposed method correctly detects fault type and in most of cases locates fault point within error of 1%.

Figure 6 depicts the phasor angle captured by four closest PMUs to the fault point of case 6 from Table I (to keep it readable). From Figure 7, it can be seen that the electromechanical wave oscillation following the fault (a-g with 20Ω at 0.9 pu from bus 19) on line 19-20 is first detected at bus 21 at t=5.43 sec and then detected at buses 15, 23 and 17, respectively.

3.4 Use-Case 2: Impact of PMU/PDC failure

Capability of deploying virtual PMUs using the SIL testbed makes it viable to study effect of unavailability of PMU streams on evaluation of the FL method. The average error of the method vs. total number of out of

Table I. FL Results under Different Fault Specification

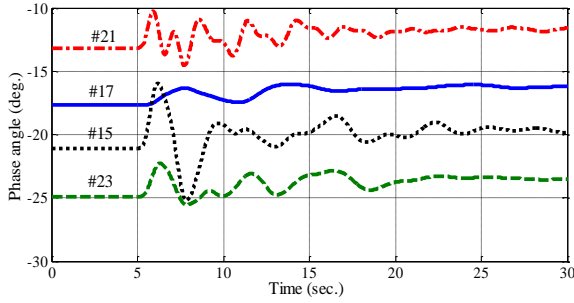| Case no.	Faulty line	Fault type	Fault resistance (Ω)	Fault distance (p.u.)	FL error (%)
1			1	0.1	0.73
2			1	0.5	0.59
3		a-g		0.9	0.34
4		a-g		0.1	1.23
5			20	0.5	0.92
6	19-20			0.9	0.74
7			1	0.1	0.56
8			1	0.5	0.51
9		ab-g		0.9	0.49
10				0.1	0.84
11			20	0.5	0.83
12				0.9	0.77
13			1	0.1	0.44
14			1	0.5	0.47
15		ab		0.9	0.62
16				0.1	0.75
17			20	0.5	0.67
18	100-106			0.9	0.93
19			1	0.1	0.17
20			1	0.5	0.14
21		abc-g		0.9	0.15
22				0.1	1.11
23			20	0.5	0.96
24				0.9	1.04

Figure 6. PMUs stream of buses 15, 17, 21, and 23

service PMUs in each area is depicted in Figure 7. To perform this study, once each PMU is taken out of service, an a-g fault with 1Ω resistance is inserted at the middle of 20 different lines at each of the three areas and average error percentage is used for plotting. Figure 7 shows that the method remains accurate under the circumstance that five PMUs in each area are out of service.
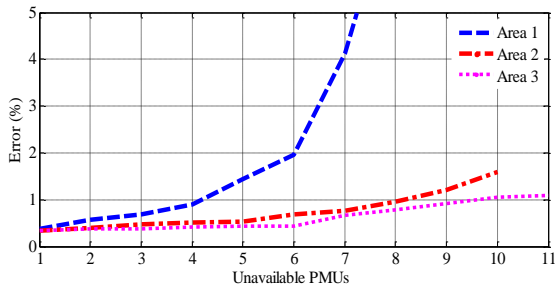

Figure 7. Fault location error vs. PMUs out of service

3.5 Use-Case 3: Impact of PMU data quality issues

The SDN controller within SIL testbed makes it possible to test robustness of the FL method vs. PMU bad data by emulating communication error including packet delay, packet loss, and channel failure. Figure 8 shows the average error of the algorithm once PMU streams are affected. In scenario 1, PMU streams in area 1 are emulated with random packet delay in the range of 20ms. An a-g fault with 1Ω resistance is inserted at the middle of 20 different lines at each of the three areas, and the average error in each area is obtained (first three columns of Figure 8 from left). It can be observed that the effect of PMU bad data is felt when the fault is occurred in the same area as the affected PMUs. The same is concluded from second and third scenarios where the PMUs in area 2 and area 3 are emulated, respectively.
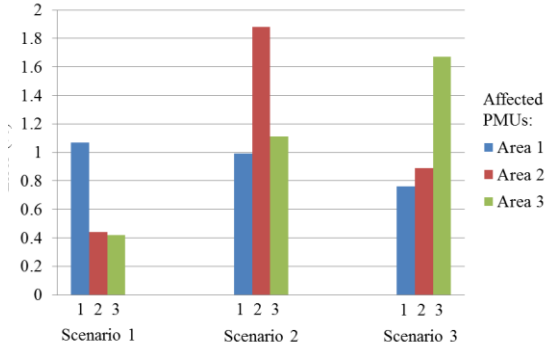

Figure 8. Effect of PMU bad data on fault location

4. HIL testbed use for developing and evaluating microgrid controller applications

Microgrids have emerged as a potential building block for the smart gird to enable effective, modular, and efficient integration of renewable energy resources in the host power system. A microgrid can operate as a standalone system, thereby increasing the resiliency and reliability of the power system in case of high-impact events. In recent years, several testbeds have been developed at universities and industries around the world. An example is our testbed that includes a transmission-level control center, a distribution-level operating center, substation and distribution feeder automation facilities, software models of renewable energy devices, and smart meters.

This section discusses the recent additions to this testbed to allow hardware-in-the-loop real-time simulation of distribution-level microgrid systems.

5

This tool enables evaluation of control strategies beyond what is possible with a mere software-based solution before they are implemented in the field. Otherwise, after field implementation, additional modifications and tuning can be costly.

4.1. Application development

Similar to an active distribution system, a microgrid includes several components, e.g., distributed energy resources (DER), capacitors, controllable loads, and power electronic devices. In many cases, each of these devices is controlled by a local controller [26], [27], which is supervised by a central controller [28], [29]. Design of these controllers is key to stable, reliable, and optimal operation of the system [30]. This design needs to be

 (1) Evaluated via simulation studies in tools such as MATLAB/Simulink [31], PSCAD/EMTDC [32], and DigSILENT PowerFactory [33]. In this case, both the microgrid and the controllers are implemented in the simulation environment [34].
 (2) Validated via hardware implementation. In this case, as discussed in this paper, the control algorithm is implemented in the same physical hardware that will eventually implement the controllers in the field.

The solution developed for this application is discussed in the following subsections.

4.2. Testbed setup

Figure 2 (on page 2) shows the schematic diagram of the developed software-based hardware-in-the-loop simulation platform. This platform has four main components: 1) a power system simulator, 2) a hardware interface, 3) a physical controller, and 4) the synchronization and coordination logic. In this paper, PSCAD/EMTDC is employed for simulation of the power system due to its flexibility, high speed, extensibility, and wide acceptance in the industry for electromagnetics-type transients simulation. The physical controller in this case is the National Instrument (NI) cRIO. NI cRIO is a robust, industry-grade controller capable of executing very fast control commands in its FPGA or efficient processing in its CPU. Since NI cRIO is used to implement the controller logic, the natural choice for the interface is LabVIEW (also developed by NI). LabVIEW interfaces to a data acquisition (DAQ) module that communicates with the external controller. However, PSCAD and LabVIEW cannot natively communicate with each other. Therefore, text files are employed as the interface media between these two software tools. Each measurement is written to a separate file. A custom PSCAD component (Figure 9) reads from these text files the data written by LabVIEW; similarly, another custom PSCAD component writes to another set of text files, which are then read by LabVIEW. Other methods of interfacing, e.g., using ports, can be employed for achieving an even higher speed of communication; however, this work does not further investigate their application. LabVIEW reads the PSCAD output files and writes their contents to the output channels of the DAQ module. The external controller then reads the data from the DAQ module. While the read/write operations on a file add a certain overhead to the simulation, this overhead is accounted for using the synchronization algorithm as discussed below.

Figure 10 shows the timeline for real-time operation enforcement. Real-time simulation is enforced by ensuring that PSCAD runs neither faster nor slower than real time. To avoid slower-than-real-time simulation, based on the available hardware, the simulation time step and the plot time step of PSCAD
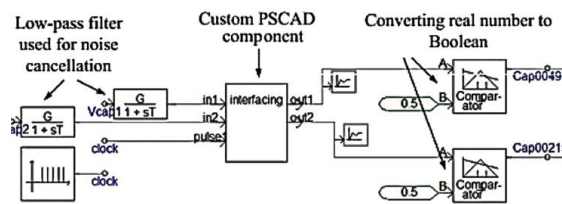

Figure 9. Custom PSCAD component for interfacing

NI-cRIO continually implements the control algorithms and sends and receives data in every time step

LabVIEW continually reads the last updated (by PSCAD) file and writes the last updated (by NI-cRIO) data to file (unless locked by PSCAD
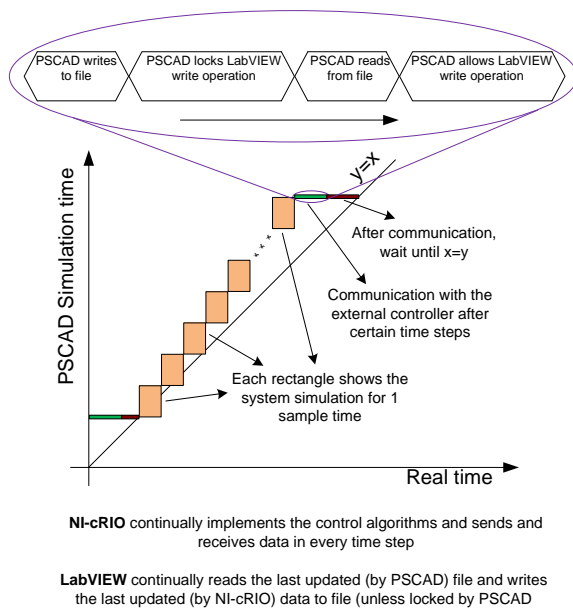
Figure 10. Timeline of the proposed real-time simulation

are selected sufficiently large and the rate of communication with the controller device (that is, read/write operations) is selected sufficiently low. To avoid faster-than-real-time simulation, a Fortran code compares the simulation time with the real time and introduces a delay if the simulation time is ahead of real time. (Fortran language is used because it is the native programming language for developing new components in PSCAD; in general other programming languages, including MATLAB and C, can also be used and linked to PSCAD.) After a certain number of simulation time steps, PSCAD communicates with the controller device. After the communication process, the simulation time and the real time are compared and the algorithm mentioned earlier is called to enforce real-time simulation.

4.3 Use-Case 1: Validation of Real-Time Simulation

To evaluate the performance of the proposed software-based HIL real-time simulator, an experimental setup is developed. As shown in Figure 11, the power system is simulated in PSCAD (right hand side of the computer screen), which is run side by side with LabVIEW (left side of the computer screen). PSCAD communicates with LabVIEW via text files, and LabVIEW communicates with the physical controller (NI cRIO) via DAQ modules. The oscilloscope is used to capture the measured waveforms. Figure 12 shows the test microgrid, which includes three switched loads and two switched capacitors. The loads can be manually switched on and off. The control objective is to maintain the voltages of the buses of capacitors C1 and C2 within the specified
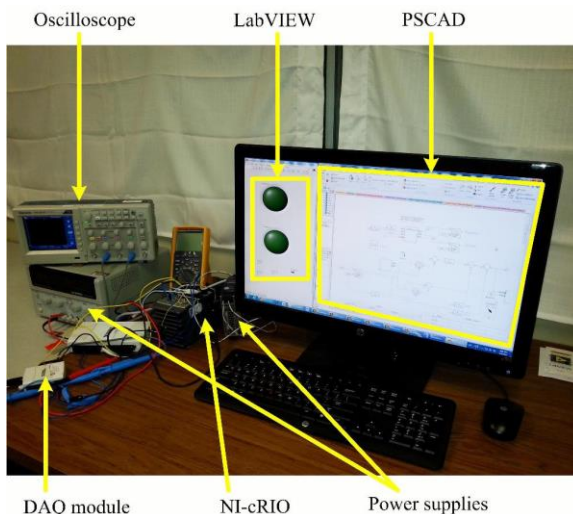

Figure 11. Setup of the proposed software-based HIL real-time simulation

limits by appropriate capacitor switching when the loads change. This logic is implemented in the NI cRIO controller.

Figure 13 shows the difference between the simulation time and the real time for the test microgrid without and with real time enforcing scheme. Without real-time enforcement, the simulation runs faster than the realtime and the difference between the two increases linearly with time. With the proposed real-time enforcement scheme, the difference between the real time and the simulation time is always maintained around zero.
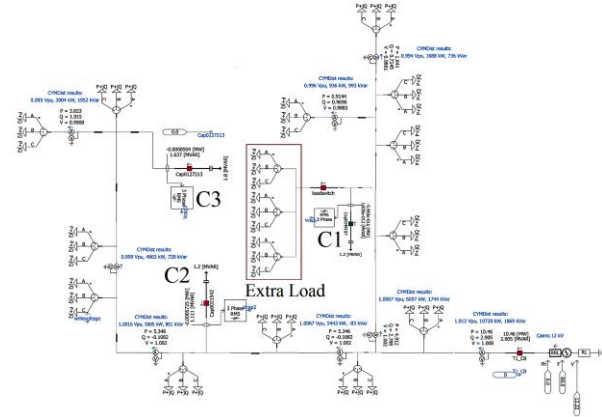

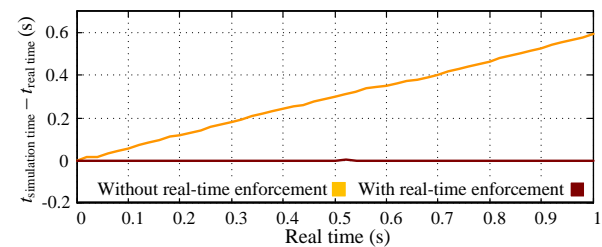**Figure 12. Test microgrid in grid-connected mode**

Figure 13. Difference between the simulation time and the real time of a sample simulation case study without and with the proposed real-time enforcing scheme.

4.4 Use-Case 2: Maintaining Voltage at Capacitor Buses with Load Switching

In this scenario, the ability of the proposed HIL architecture as well as the control system to maintain the voltages of the system within the desired levels as system loads change is evaluated. To observe the physical signals, as shown in Figure 14, an oscilloscope is used to monitor the desired simulation variables. Figure 15 shows the PSCAD simulation results without and with the controller device interfaced to the simulator. Prior to switching the loads on (at $t = 70$ s), the bus voltages are within the defined limits ($V_{C_1} \in [0.98, 0.995]$, $V_{C_2} \in [0.99, 0.998]$). When the load increases, the voltages of both buses decrease.
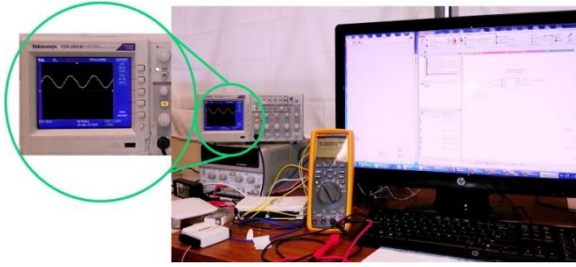
7

Figure 14. Using an oscilloscope for observing the single phase voltage of a bus
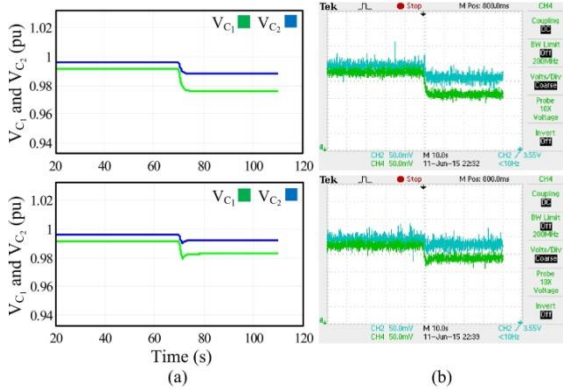

Figure 15. HIL real-time simulation results: (a) readings of PSCAD plots; (b) measurements of the physical oscilloscope. From top to bottom: Voltages of the capacitor buses when the external controller is not interfaced to the simulation and both capacitors are switched off; and voltages of the capacitor buses when the external controller is interfaced to the simulation.

Without the external controller, the voltages of both buses decrease significantly, as shown in Figure 15(a)-top. With the external controller interfaced to PSCAD, when the feeder load increases, the controller regulates the voltages of these buses, Figure 15(a)-bottom. Figure 15 (b) shows the voltages of the same buses as measured by an oscilloscope. Figures 15(a) and (b) use the same scales for horizontal and vertical axes. Equivalence of the time scales of PSCAD plot (simulation time) and the oscilloscope (real time) validates the effectiveness of the proposed real-time enforcement scheme.

5. CPS testbed use for developing and evaluating cybersecurity applications

The PowerCyber has automated front-end and back-end to support remote access to the testbed. The experimentation framework has been implemented using story-board based approach that enables defining both power and cyber system topologies and configuring both attacks and defense measures. Figure 16 shows the web-based front-end of the testbed for

remote access [35]. This implementation facilitates ease of use for a versatile community of users with different expertise and also serves as an educational platform that allows users to learn about the importance and criticality of cyber security of critical infrastructures such as smart grid. The remote access framework supports the following story board constructs focusing on WAMPAC applications.

Figure 16. Front-end of PowerCyber Testbed

5.1 Use-Case 1: Cascading outage through a coordinated cyber attack on power system's wide-area protection scheme [21]

In this scenario (depicted in Figure 17), the attack involves a combination of two coordinated attack actions on a power system protection scheme known as Remedial Action Scheme (RAS). Typically, RAS is intended to take specific protective measures to prevent the spread of large disturbances under heavy system loading conditions. However, an attacker could intelligently trigger the operation of this RAS by creating a data integrity attack on unencrypted communication between the substation and the control center (or by performing a replay attack if the communication channel is encrypted) that uses the DNP3 protocol. In order to create a cascading outage, the attacker also blocks the communication between the protection relays that are involved in the RAS through a targeted Denial of Service (DoS) attack on one of the protection controllers. In this example, first line outage is caused by tripping the relay between Bus B7-B5 and simultaneously a DoS attack is performed on the RAS Controller or its communication channel
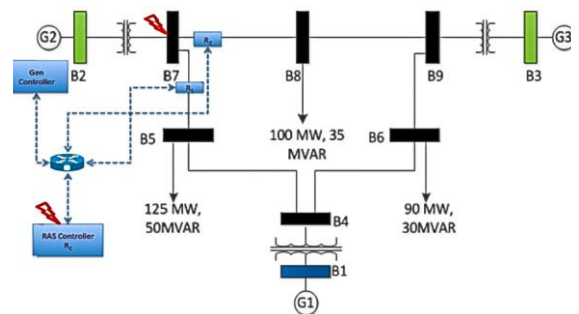

Figure 17. Coordinated attack on RAS (9-bus)

8

preventing its "ramp down" command not reaching Generation Controller of G2. This prevents the successful operation of the RAS and in turn initiates secondary protection to be tripped to avoid thermal overload on the impacted transmission line (B7-B8). As a result of this coordinated attack involving data integrity attack to trip a breaker and a DoS attack on RAS communications, the overall system frequency is also affected as it causes the islanding of a generator (G2) from the rest of the system.

5.2 Use-Case 2: Manipulating Automatic Generation Control (AGC) measurements and/or controls to affect system frequency [36]

In this scenario, the attack involves a stealthy manipulation of measurements/controls used in Automatic Generation Control (AGC) algorithm to destabilize and affect the frequency of the power grid. This attack is a version of the classic Man-In-The-Middle (MitM) attack, where the attacker intercepts the communication between the control center and the remote substations (forward communication) and chooses to stealthily modify the frequency and/or tie-line measurements going to the control center, or the AGC control commands going to the generating stations (reverse communication). For example, manipulating the forward communication is achieved by executing an ARP (Address Resolution Protocol) poisoning attack first, which tricks the remote substation to forward the data to the attacker before sending it to the external gateway at the control center. The attacker then selects targeted information (measurements) that is to be manipulated and modifies it maliciously using custom attack scripts and forwards it to the control center gateway. As a result of this manipulation, the AGC algorithm ends up computing wrong Area Control Error (ACE) values that cause the generators to ramp up or ramp down in the wrong direction. As a result, there will be a steady deviation in system frequency, which will trigger shedding of some loads in an attempt to restore the frequency. In summary, a sustained stealthy attack could potentially lead to a major load shedding, which in turn could also trigger cascading events.

The testbed has been used for impact characterization of AGC algorithm over a multi-area system and also for evaluating the effectiveness of mitigation algorithms, such as firewalls, intrusion detection systems, and model-based anomaly detection that utilizes cyber-physical system properties.

6. Conclusions

As a result of the work presented, the following are the contributions:

- It has been demonstrated that the use of testbeds offers new opportunities to develop more robust solutions that can be evaluated under realistic conditions well ahead of their implementation in a production system, which saves the time and cost of development and deployment.
- SIL testbed has been invaluable in testing new FL application since it enabled end-to-end evaluation of the various implementation impacts on the FL error such as power system scale, management of PMU/PDC measurement, and handling of data quality issues.
- HIL real-time simulation can be a valuable step, after offline simulation, when evaluating the performance of controllers within a microgrid, which otherwise is hard to evaluate using only the conventional modeling and simulation methods.
- CPS security testbeds are enabling technologies that have the potential to accelerate R&D, education and training in smart grid security by providing realistic platforms for system-scale as well as component-specific experiments pertaining to vulnerability assessment, impact analysis, security validations, attack-defense evaluations, and forensic analysis.
- The testbeds also enable bridging the gap between academic research and industry practice and can contribute to workforce development in this growing area of importance.
- From a technical point of view, architecting a modular CPS testbed for smart grid with support for scalability and programmability is in its early stages and hence significant further research needs to be done.

7. References

[1] V. Hamidi, K. S. Smith, R. C. Wilson, "Smart Grid technology review within the Transmission and Distribution sector", *IEEE PES (ISGT Europe)*, Gothenburg, 11-13th Oct., 2010.

[2] American Recovery and Reinvestment Act of 2009, "Synchrophasor Technologies and their Deployment in the Recovery Act Smart Grid Programs", August 2013.

[3] C. Battistelli, "Generalized microgrid-to-smart grid interface models for vehicle-to-grid", *IEEE PES ISGT USA*, Washington, 24-27th Feb., 2013.

[4] Public Interest Energy Research (PIER) Program Interim Project Report, "Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks", May 2012.

[5] R. M. Reddi and A. K. Srivastava, "Real time test bed development for power system operation, control and cyber security," *in Proc. North Amer. Power Symp. (NAPS)*, Sep. 26–28, 2010, pp. 1–6.

[6] S. P. Carullo, C. O. Nwankpa, "Interconnected power systems laboratory: A computer automated instructional facility for power system experiments", *IEEE Trans. on Power Systems*, vol. 17, no. 2, pp. 215–222, May 2002.

[7] P. Meinhardt, "Time Synchronized End to End Testing Using IRIG-B," *IET 9th International Conf. on Developments in Power System Protection,* March 2008.

[8] S. Turner, "End-to-end testing transmission line protection schemes and double-ended fault locators," *66th Annual Conference for Protective Relay Engineers,* College Station, TX, 2013.

[9] A. Apostolov, B. Vandiver, "End to End Testing - What Should You Know?," *67th Annual Conference for Protective Relay Engineers*, College Station, TX, 2014.

[10] V. Salehi, A. Mohamed, A. Mazloomzadeh, O. A, Mohammed, "Laboratory-Based Smart Power System, Part I: Design and System Development", *IEEE Trans. on Smart Grid*, vol. 3, no. 3, pp. 1394-1404, Aug. 2012.

[11] X. Wu, S. Lentijo, A. Monti, "A Novel Interface for Power-Hardware-In-the-Loop Simulation, *IEEE COMPEL 2004*, Urbana-Champaign, IL, August 2004.

[12] A. Monti, F. Ponci, et. al, "Hardware-in-the-Loop Testing Platform for Distributed Generation Systems", *Journal of Energy Tech. & Policy*, vol. 5, no. 2, 2007.

[13] H. G. Aghamolki, Z. Miao, L. Fan, "A Hardware-in-the-Loop SCADA Testbed", *North American Power Symposium (NAPS),* Charlotte, USA, 4-6 Oct., 2015.

[14] A. V. Prokhorov, A. S. Gusev, and Y. S. Borovikov, "Hardware-in-the-Loop Testbed Based on Hybrid Real Time Simulator", *4th IEEE PES Innovative Smart Grid Tech. Europe (ISGT Europe)*, October 6-9, 2013.

[15] H. Li, et. al, "Development of a unified design, test, and research platform for wind energy systems based on hardware-in-loop realtime simulation", *IEEE Trans. on Ind. Electr.*, vol. 53, no. 4, pp. 1144-1151, Aug. 2006.

[16] M. J. Stanovich, I. Leonard, K. Sanjeev, M. Steurer, et. al, "Development of a Smart-Grid Cyber-Physical Systems Testbed", *Innovative Smart Grid Technologies (ISGT)*, 24-27 Feb., Washington, USA, 2013.

[17] U. Adhikari, T. Morris, S. Pan, "A CyberPhysical Power System Test Bed for Intrusion Detection Systems", *IEEE PES General Meeting*, 27-31 July, USA.

[18] A. Esmaeilian, M. Kezunovic, "Fault location using sparse synchrophasor measurement of electromechanical wave oscillations", *IEEE Trans. on Power Delivery*, vol. pp, no. 99, Dec. 2015.

[19] S. Ziaeinejad and A. Mehrizi-Sani, "Software-based hardware-in-the-loop real-time simulation of distribution systems," in *IEEE Power and Energy Soc. General Meeting (PESGM 16)*, Boston, MA, Jul. 2016.

[20] S. Sridhar, A. Hahn, M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. of the IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

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

[22] ISERINK platform for Cyber Defense Competitions, Iowa State University, 2015. URL: http://www.iserink.org/

[23] E. O. Shweitzer, D. Whitehead, G. Zweigle and K. G. Ravikumar, "Synchrophasor-based power system protection and control applications", *Proceedings of the International Symposium on Modern Electric Power Systems (MEPS)*, Wroclaw, 20-22 Sept., 2010.

[24] P. Dutta, A. Esmaeilian, M. Kezunovic, "Transmission-Line Fault Analysis Using Synchronized Sampling," *IEEE Trans. Power Delivery*, vol. 29, no. 2, April 2014.

[25] A. Esmaeilian, M. Kezunovic, "Impact of Electromechanical Wave Oscillations Propagation on Protection Schemes," *Electric Power Systems Research*, pp. 1-7, Jan. 2016.

[26] I. Roytelman and V. Ganesan, "Modeling of local controllers in distribution network applications," *IEEE Trans. Power Del.,* vol. 15, no. 4, pp. 1232-1237, 2000.

[27] I. Dzafic, R. Jabr, E. Halilovic, and B. Pal, "A sensitivity approach to model local voltage controllers in distribution networks," *IEEE Trans. Power Syst.,* vol. 29, no. 3, pp. 1419–1428, May 2014.

[28] I. Roytelman, V. Ganesan, "Coordinated local and centralized control in distribution management systems," *IEEE Trans. Power Del.* vol. 15, no. 2, pp. 718–724, Apr. 2000.

[29] B. Robbins, C. Hadjicostis, and A. Dominguez-Garcia, "A two-stage distributed architecture for voltage control in power distribution systems," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1470–1482, May 2013.

[30] H. Hatta, S. Uemura, H. Kobayashi, "Demonstrative study of control system for distribution system with distributed generation," in *Power Syst. Conf. Expo.*, Seattle, Mar. 2009.

[31] MathWorks, Inc. (2015) Simulink user's guide. [Online]. Available: http://www.mathworks.com/help/pdf_doc/simulink/sl_using.pdf

[32] Manitoba HVDC Research Centre. (2010) User's guide on the use of PSCAD. [Online]. Available: https://hvdc.ca/uploads/ck/files/reference_material/PSCAD_User_Guide_v4_3_1.pdf

[33] DIgSILENT GmbH. (2015) DIgSILENT powerfactory 15. [Online]. Available: http://www.digsilent.de/tl_files/digsilent/files/powerfactory/PowerFactory15/WhatsNew_PF150.pdf

[34] J. Mahseredjian, V. Dinavahi, and J. Martinez, "Simulation tools for electromagnetic transients in power systems: overview and challenges," *IEEE Trans. Power Del.*, vol. 24, no. 3, pp. 1657–1669, Jul. 2009.

[35] A. Ashok, P. Wang, M. Brown, and M. Govindarasu, "Experimental evaluation of cyberattacks on automatic generation control using a cps security testbed," *in Proc. PES General Meeting*, 2015 IEEE, July 2015.

[36] S. Krishnaswamy, "Accessible Remote Testbed for Cyber Physical Systems Security of the Smart Grid," M.S. Thesis, Iowa State University, Summer 2016.