A Hardware-in-the-loop Experimental Platform for Power Grid Security

Mr. James Dylan Kollmer

James Kollmer is currently a second year master's student in Electrical and Computer Engineering at Temple University. His research is focused on networked control systems and more specifically, Smart Grid resiliency and protection schemes via control theory applications. He is particularly interested in power systems, power electronics, and resilience control applications. Before coming to Temple University, he graduated from East Stroudsburg University and Temple University with a bachelor's in physics and Electrical engineering. He is currently finishing up his Master's thesis and works at the Naval Surface Warfare Center Philadelphia Division. He can be contacted at: james.kollmer@temple.edu

Dr. Saroj K Biswas, Temple University

Saroj Biswas is a Professor of Electrical and Computer Engineering at Temple University specializing in electrical machines and power systems, multimedia tutoring, and control and optimization of dynamic systems. He has been the principle investigator of a project for the development of an intelligent tutoring shell that allows instructors create their own web-based tutoring system. His current research focuses on security of cyber-physical systems based on multiagent framework with applications to the power grid, and the integration of an intelligent virtual laboratory environment in curriculum. He is an Associate Editor of Journal of Industrial and Management Optimization, and is a member of IEEE, ASEE, and Sigma Xi.

Dr. Li Bai, Temple University

Dr. Li Bai is a Professor in the ECE department, Temple University. He received his B.S. (1996) from Temple University, M.S. (1998) and Ph.D. (2001) from Drexel University, all in Electrical Engineering. He was a summer research faculty in AFRL, Rome, NY, during 2002–2004 and the Naval Surface Warfare Center, Carderock Division (NSWCCD), Philadelphia, PA, during 2006–2007. His research interests include video tracking, level 2+ information fusion, array signal processing and multi-agent systems, wireless sensor network and dependable secure computing. His research has been supported by Office of Naval Research, Department of Transportation, U.S. Department of Commerce's Economic Development Administration (EDA), National Science Foundation, U.S. Army and Exxon Mobil, etc. Also, Dr. Bai served as the Chair of the IEEE Philadelphia Section in 2007 and was Young Engineer of the Year in Delaware Valley, IEEE Philadelphia Section in 2004.

Dr. Arif I. Sarwat, Florida International University

Arif I. Sarwat (M'08) received his M.S. degree in electrical and computer engineering from University of Florida, Gainesville. In 2010 Dr. Sarwat received his Ph.D. degree in electrical engineering from the University of South Florida. He worked in the industry (SIEMENS) for nine years executing many critical projects. Currently, he is an Associate Professor at the Department of Electrical and Computer Engineering at Florida International University (FIU), where he leads the Energy, Power and Stainability (EPS) group. His significant work in energy storage, microgrid and DSM is demonstrated by Sustainable Electric Energy Delivery Systems in Florida. His research areas are smart grids, Electric Vehicles, high penetration renewable systems, cyber-physical systems, power system reliability, large scale distributed generation integration, large scale data analysis, cyber security, and vehicular technology. Dr. Sarwat is the recipient of the NSF CAREER award in 2015.

Walid Saad, Virginia Tech

Walid Saad received his Ph.D degree from the University of Oslo in 2010. Currently, he is an Associate Professor at the Department of Electrical and Computer Engineering at Virginia Tech, where he leads the Network Science, Wireless, and Security (NetSciWiS) laboratory, within the Wireless@VT research group. His research interests include wireless networks, machine learning, game theory, cybersecurity, unmanned aerial vehicles, and cyber-physical systems. Dr. Saad is the recipient of the NSF CAREER

award in 2013, the AFOSR summer faculty fellowship in 2014, and the Young Investigator Award from the Office of Naval Research (ONR) in 2015. He was the author/co-author of six conference best paper awards at WiOpt in 2009, ICIMP in 2010, IEEE WCNC in 2012, IEEE PIMRC in 2015, IEEE SmartGridComm in 2015, and EuCNC in 2017. He is the recipient of the 2015 Fred W. Ellersick Prize from the IEEE Communications Society and of the 2017 IEEE ComSoc Best Young Professional in Academia award. From 2015-2017, Dr. Saad was named the Stephen O. Lane Junior Faculty Fellow at Virginia Tech and, in 2017, he was named College of Engineering Faculty Fellow. He currently serves as an editor for the IEEE Transactions on Wireless Communications, IEEE Transactions on Communications, IEEE Transactions on Mobile Computing, and IEEE Transactions on Information Forensics and Security.

A HARDWARE-IN-THE-LOOP EXPERIMENTAL PLATFORM FOR POWER GRID SECURITY

Abstract

This paper presents the development of a hardware-in-the-loop testbed for a three-bus power grid interfaced with a simulated networked control system (NCS) for studying cyber security threats and their possible impacts on the power grid. The three-bus grid consists of two generator buses, configured as slack bus (constant voltage and angle) and PV bus (constant power and constant voltage), and a load bus (PQ bus). The synchronous generators are driven by dynamometers serving as prime movers, and the field circuits controlled by insulated gate bipolar junction transistor (IGBT) DC/DC choppers. The load bus operates switchable resistors, capacitors, and inductors that are connected to the generator buses through transmission lines. The simulated NCS is implemented on an Opal real-time (Opal-RT) platform, which is a PC/FPGA based real-time simulator that can integrate hardware with software simulations, commonly referred to as hardware-in-the-loop (HIL). In general, HIL setups have the advantage that physical elements under test interact in real time with a simulated model of a large scale system and provide a better insight of performance of both the physical system and the controller. In this HIL experiment, the data acquisition unit (DAQ), and the controller are both implemented on the Opal-RT platform. The controller determines the duty cycle of the pulse width modulated (PWM) signals applied to the gate of the IGBT which controls the voltage applied the generator field circuits, thus producing desired terminal voltages of the generators. Experimental results are presented that show the effects of cyber-attacks on a generator control system. A baseline for the behavior of the three-bus system is first established by operating the generator under various load conditions for which the controller maintains the desired terminal voltage. Then, a series of denial-of-service (DoS) attacks in the feedback loop were launched. With no attack prevention mechanism in place, the developed experimental platform provides a facility to observe and evaluate the impacts of various cyber-attacks on a real physical microgrid. The developed HIL platform allows students to experiment with various cyberattack scenarios, defense strategies, and control algorithms due to the reconfigurable nature of the HIL system.

Keywords

Hardware-in-the-loop, Networked control system, synchronous generator control, data acquisition system, cyberattacks.

1. Introduction

The U.S. power grid forms the core of all infrastructures, defense, and commerce in the United States which makes it a prime target [1]-[4] for cyber terrorism. In recent years, there have been many incidents of cyberattacks on the power grid all over the world including the Ukrainian grid cyberattack [5] in December 2015 that disrupted power supply to over 230 thousand customers for up to 6 hours. Whether or not it is possible to prevent cyberattacks on the grid is debatable,

therefore it is necessary to develop control system tools that could keep the smart grid stable and operational in the events of such attacks. Over the last decade, there have been significant efforts on the development of security hardware and software for industrial control systems, nevertheless a general consensus is that the power sector is not yet prepared to combat cyberattacks [2], [7]-[10] and [27]. This research investigates the development of a hardware-in-the-loop attackable and observable experimental testbed that can be used to investigate the effects of cyberattacks on the grid, and develop and test security countermeasures to minimize any detrimental effects that may destabilize the overall grid.

Replicating a realistic power grid in the laboratory using physical hardware is difficult and expensive. This primarily relegates the power systems security research to the domain of simulation experiments. One example of such simulation platforms is the Grid Game [11], an interactive simulation platform developed at Idaho National Laboratory that is played between two players in which the 'grid operator' attempts to maintain a constant grid frequency by taking defensive actions in the events of attacks launched by 'cyberattackers'. Similarly, the Aurora Generator Test at the INL in 2007 is probably the earliest experimental demonstration that showed the effects of a possible cyberattacks on the power grid.

In recent years, hardware-in-the-loop (HIL) experiments [16]-[26] have drawn considerable interest as a way of testing physical hardware in a real world environment. In HIL experiments, physical elements under test interact in real time with a simulated model of a large scale system and/or a controller and data acquisition system through appropriate analog and digital interfaces, and provides a better insight of performance of both the physical system as well as the controller. Examples of HIL experiments include interaction of a voltage source converter with an electric ship power grid [16], control of inverters and buck converters [21], evaluation of an industrial level generator excitation control system with the turbine-generator system [22], photovoltaic generation and power interface [23], active power control of wind power plant [24], MVDC integrated power system for electric ships [25], and many more. Various requirements and characteristics for the implementation of HIL experiments including bandwidth, accuracy, and stability have been outlined in several recent references (e.g., see [18], [19], [20], and [26]).

The main contribution of this paper is the development of a novel experimental HIL platform for demonstrating the effects of cyberattacks on a three-bus power system. The cyber component of the HIL platform is based on a real-time PC/FPGA-based simulator Opal-RT, and the physical component of a three-bus power grid based on LabVolt EMS8000 series actual power generators and loads. The three-bus grid is configured as a slack bus (constant voltage and angle), a PV bus (constant power and voltage), and a PQ bus or load bus of switchable resistors, inductors and capacitors. Two synchronous generators are connected to the slack bus and the PV bus, respectively, with the slack bus generator configured for constant frequency. The instrumentation layer of the system includes various sources and sensors within the OP8660 HIL controller and data acquisition interface that measure voltages and currents at all buses, and speed of the synchronous generators. The computational engine of the HIL system implemented in the Opal-RT includes a control algorithm for the generator field circuit, data processing, computation of real and reactive power, and other pertinent quantities, and for launching simulated cyberattacks. The feedback loop is completed through the OP8660 HIL controller and data acquisition interface that sends the control signal from the Opal-RT to the gate of the IGBT which ultimately controls the applied voltage of the generator field coil, and hence the induced EMF.

Experimental results are presented that include normal operating state of the three bus grid, and that of the system under denial-of-service attacks. A baseline for the behavior of the three-bus grid is first obtained by running the system under normal operating conditions. This experiment demonstrated the effectiveness of the controller in maintaining stability of the grid and desired voltages at various buses as the system load at PQ bus was varied. Then, a series of (simulated) denial-of-service attacks were launched on the controller of the PV bus generator by increasing the probability of packet drop in the network, modeled by an i.i.d. Bernoulli process. With no attack prevention mechanisms in place, the platform provides a facility to observe and evaluate the impacts of various cyberattacks on a real, physical power generator.

The rest of the paper is organized as follows. Section 2 presents the development of the HIL hardware platform using LabVolt EMS8000 series equipment and Opal-RT real time simulator. Experimental results of cyberattacks on the three-bus system are presented in Section 3. Results of a laboratory demonstration to a group of undergraduate students are presented in Section 4 followed by concluding remarks in the Section 5.

2. HIL-Cyber Physical System

The HIL simulation is based on a hybrid configuration of a cyber system and a physical system that interact with each other through digital and analog input/output (I/O) signals. The cyber system uses the computing power and flexibility of a real time digital simulator, such as Opal-RT or RTDS, that receives feedback signals from the connected physical system. Figure 1 shows the high-level view of the HIL testbed for closed-loop control of a three-bus electrical grid which consists of two generator buses and a load bus. The load is shared by the two synchronous generators, and as the load changes, the terminal voltage of the generators also changes accordingly. The generator terminal voltages are controlled by adjusting the field current using a controller. The feedback loop is completed through the OP8660 for data transmission between the generator terminals to the controller on the Opal-RT, and between the controller and the field coil. This makes the closed loop system vulnerable to cyberattacks since a cyber intruder can easily initiate a data attack or a denial-of-service (DoS) attack in the generator control system.

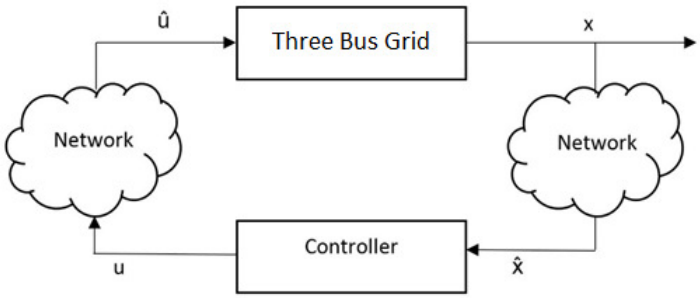

Figure 1 Schematic of Closed Loop NCS System.

2.1 The Cyber System: Opal-RT Simulator

The developed hardware-in-the-loop system uses an Opal-RT real-time processor for implementation of the controller for the two generators. Opal-RT is a PC/FPGA-based real-time simulator for the hardware-in-the-loop experimental platform presented in this paper. The specific

Opal-RT hardware platform in the experiments shown in Figure 2 is an OP5600 in conjunction with an OP8660 HIL controller and data acquisition interface. The OP5600 is equipped an Intel Xeon CPU and a Xilinx Spartan-3 FPGA. The simulations are executed on the CPU and the FPGA handles the hardware interface and is reconfigurable to suit the user's needs. The OP8660 is a user-friendly interface meant for easy integration as the I/O connections options are either banana cables or DB9 cables. The OP8660 is especially good at interfacing with the LabVolt series of equipment.

Figure 2 OP5600 and OP8660 from left to right.

The process of utilizing the Opal-RT platform consists of first creating a Matlab/Simulink model to meet the user's goals (in this a case a controller and data acquisition system). The model is then configured to communicate with the specific hardware needed to properly execute the HIL setup. Once the hardware is connected to the Opal-RT platform and the system is properly configured, the user can run the model on the Opal-RT and gather data for analyzing and controlling the HIL experimental setup.

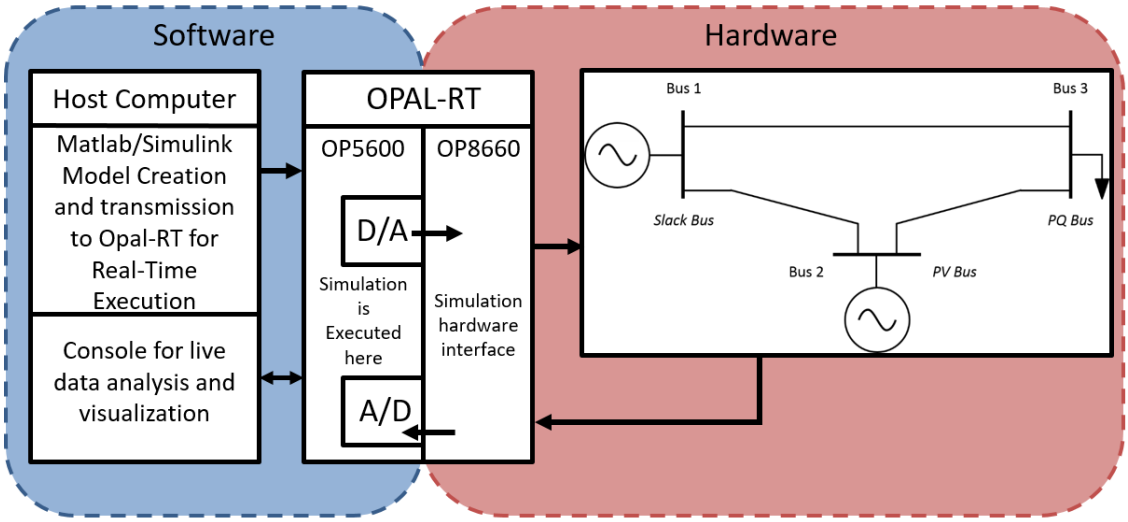

Figure 3 Opal RT High Level Control Loop

The setup specific to this application as shown in Figure 3 portrays how the overall HIL creation, setup, and operation is accomplished. The initial step in the process is to create and build the Matlab/Simulink model on the host computer and then send the built model to the Opal to be executed. Another aspect of the host computer in the HIL setup is to act as the user interface console for the Opal whilst the model is executed. The host computer console displays information such as voltages, currents, and control signals, and send commands such as turn the controllers

on/off or change control gains. The model is executed in real-time on the OP5600. The communication between the OP5600 and the hardware is accomplished with the OP8660 HIL controller and data acquisition interface which transmits the control signals to the hardware and receives the voltage and current measurements and converts them to a format that the analog to digital converter on the OP5600 can interpret.

2.2 The Physical System: Three-bus Network

The proposed experimental physical system is a three-bus electric network as shown in Figure 4. The developed three-bus system consists of two LabVolt EMS8000series synchronous generators driven by dynamometers. The dynamometers were configured so that the slack bus generator runs at constant speed of 1800 rpm, and the PV bus generator supplies constant power using built-in fast-acting dynamometer control systems, however the speed can vary during transients. The load bus consists of switchable RLC loads through three transmission lines as shown. The actual hardware used in the testbed is shown in Figure 5.

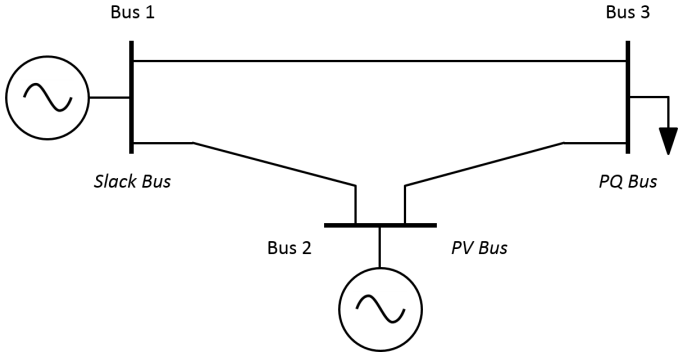

Fig. 4 Three-Bus Electrical Network.

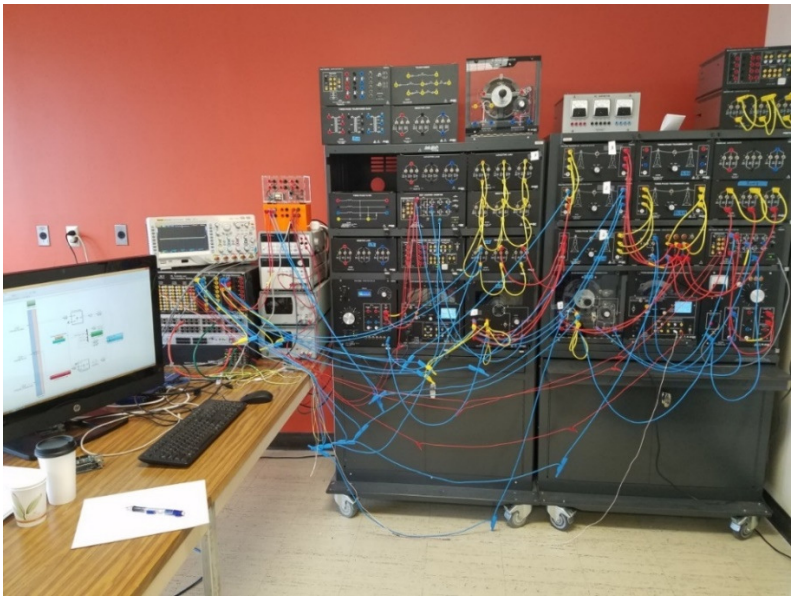

Figure 5 Experimental Setup.

The schematic of the generator field excitation system is shown in Figure 6, which consists of a PI (proportional-integral) controller and an IGBT chopper supplying the generator field coil. The IGBT chopper regulates its DC output voltage based on gate pulse supplied by the PI controller, and the corresponding field current is nearly constant because of high inductance of the field winding. The induced EMF of the generator is proportional to the duty ratio of the IGBT chopper.

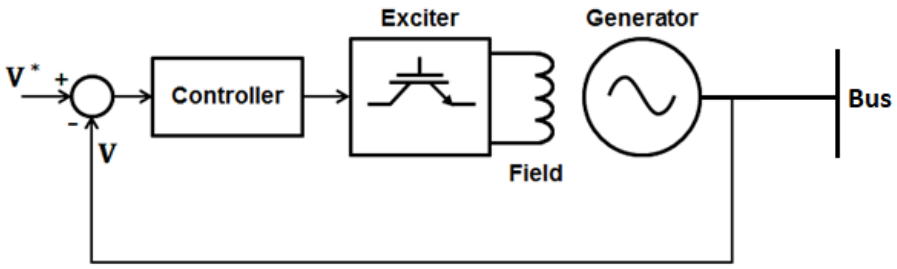

Figure 6 Generator Excitation System.

Figure 7 shows additional details on the generator field control system. The output of the PI (proportional-integral) controller is the duty cycle ratio, d, which is ideally between 0 and 1. A limiter is implemented in software to ensure that duty cycle ratio d remains between 0.02 and 0.98 which ensures the safety of the IGBT, however was not used in control design to minimize complexity. The generator field circuit is represented by a resistance R_f and an inductance L_f. The induced EMF of the generator is proportional to the field current i_f where the magnetic constant of the field coil is represented by k_f.

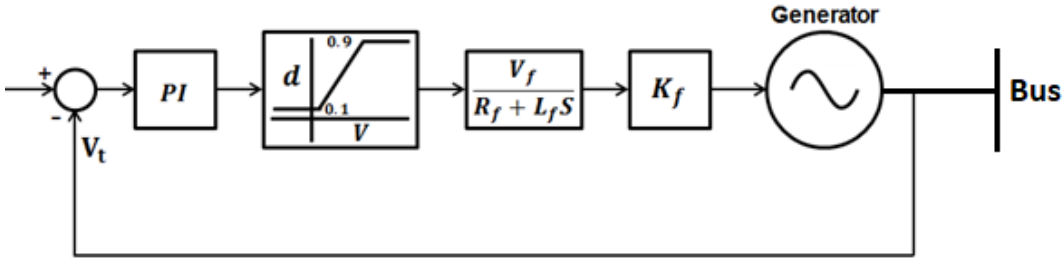

Figure 7 Block Diagram of the Generator Control System

The complete transfer function of the system was obtained by first principle modeling and experimentation as reported earlier [14]. The transfer function of the PI controller is given by

$$G_c(s) = k_p + \frac{k_i}{s},$$

where the proportional gain $k_p = 0.005$ and the integral gain $k_i = 0.1$. Performance of the closed loop system was verified by simulations and additional experiments.

3. Experimental Results

In this section, we present the results of cyberattacks on the PV bus generator control system however no cyberattacks were considered on the slack bus generator. Cyberattacks were implemented in the simulation on the Opal-RT and were targeted specifically at the generator voltage sensor data and the controller. As the (simulated) intruder intercepts the voltage sensor data, the actual data received by the controller is modified according to the attack process.

The first step of experimentation is to synchronize the two generators. The slack bus generator was first configured to run at 1800 rpm. Then the PV bus generator controller was adjusted to generate 9.375W at 75V and 1800 rpm and the dynamometer was set to run at constant torque. A LabVolt synchronizing module was then used to synchronize the two generators. For this three-bus system, the PV bus generator output remained constant (except during transients), while the balance of PQ bus load and line losses are supplied by the slack bus generator.

3.1 Baseline Performance

To validate the performance of the excitation system controllers, first, we show the closed-loop system performance running under various load conditions. After the generators were synchronized, the PQ bus loads were turned ON and OFF at various time points as marked in the Figures 8-11. Figure 8 clearly shows that the controller maintained the terminal voltage of the slack bus generator (middle window) and the PV bus generator (top window) constant as the PQ bus load was varied. Transients in the terminal voltage are however expected during the load switching as seen in Figure 8. The load bus voltage (bottom window) drops when load demand increases due to higher line voltage drop, increases when capacitive load is switched ON, which easily follows from simple circuit concepts. Opposite effect on terminal voltage at load bus is observed when inductive load is switched ON. Changes in load bus voltage were due to changes in the line voltage drop between the load bus and the other buses.

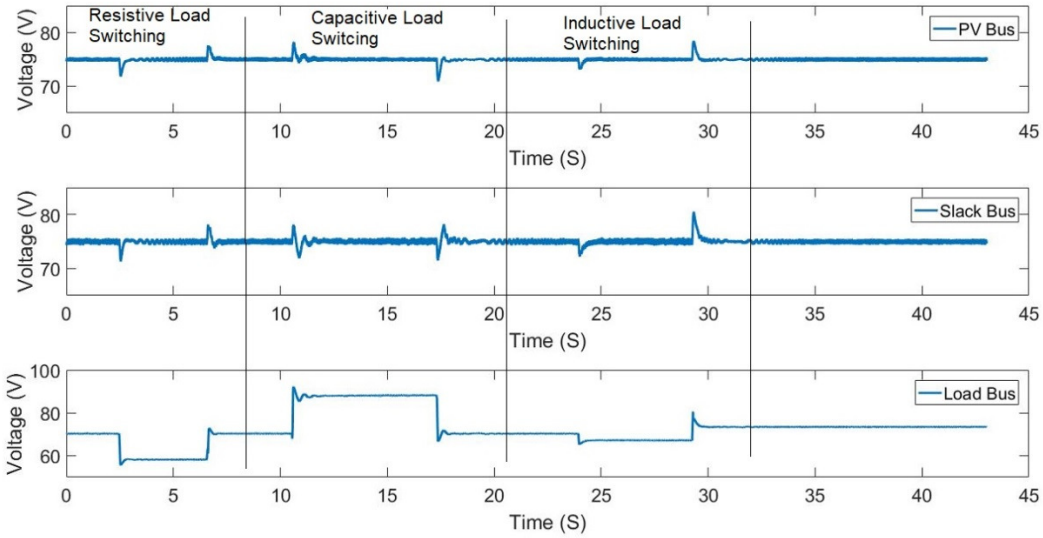

Figure 8 Bus Voltages for Load Switching.

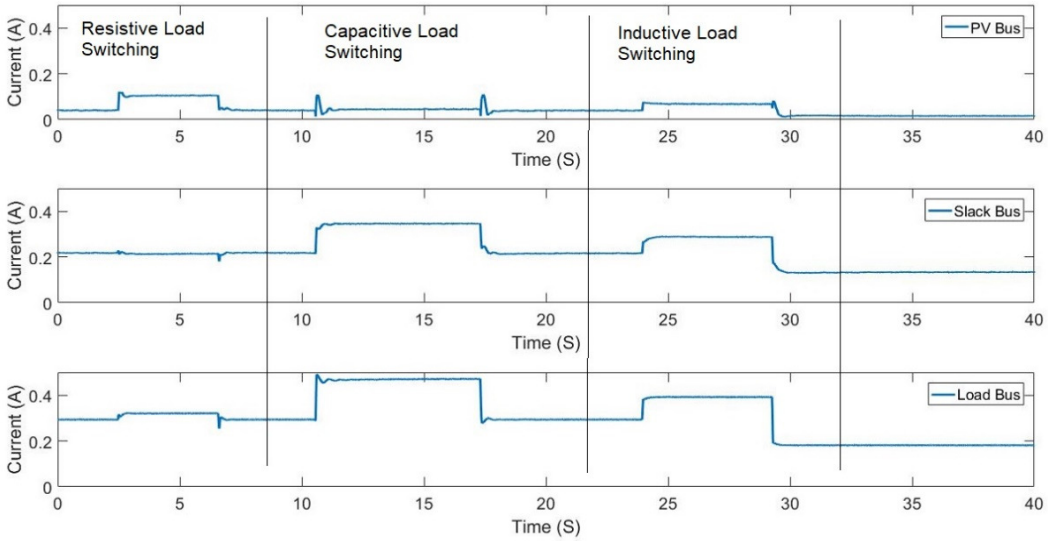

Figure 9 Bus Currents for Load Switching.

Figure 9 shows that the load current (bottom window) varies significantly with changes in load, however the current supplied by PV bus generator (top window) remained relatively constant which is expected since the PV bus generator operates as a constant torque generator producing constant output power. The slack bus generator (middle window) supplies the additional current required by the load and changes in line losses.

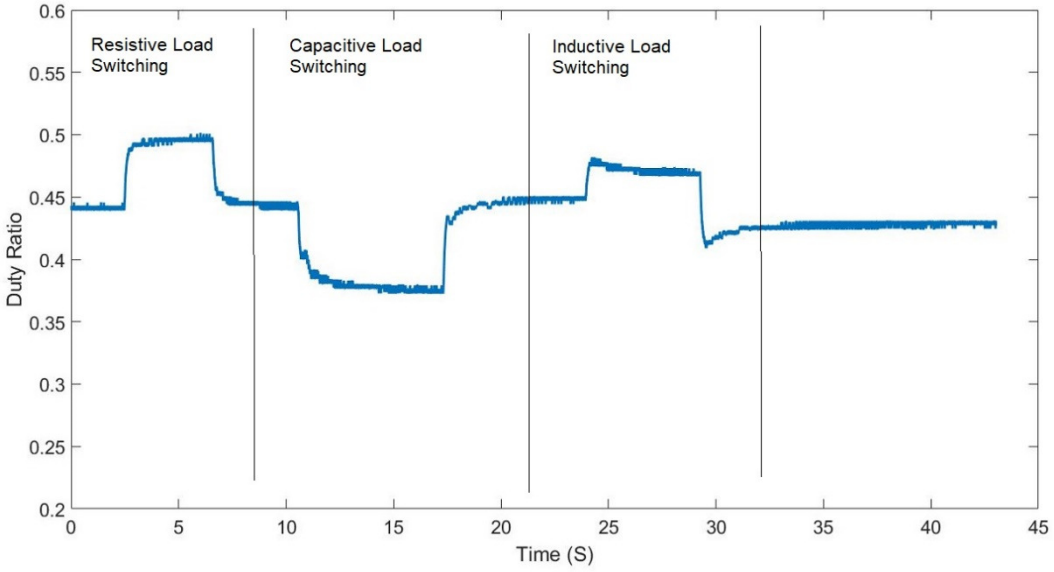

Figure 10 Duty Cycle Ratio of slack bus generator for Load Switching.

Figure 10 shows the duty cycle ratio of IGBT controller of slack bus exciter. As the generator supplies more resistive current, its generated voltage must be increased so that the terminal voltage

remains constant as signified by a higher duty cycle ratio of the IGBT controller. Recall that the induced EMF is proportional to the IGBT duty cycle ratio. For capacitive current loads, as expected the induced EMF must be decreased as seen from Figure 8 and corresponding lower duty cycle ratio of the IGBT controller. For inductive loads, a higher duty cycle ratio of the IGBT controller is required since induced EMF is expected to be higher. The duty cycle ratio of the PV bus IGBT controller remained relatively constant (not shown in the figure) except during transients because the output current of the generator remained relatively constant. Here, we recall that the PV bus generator is expected to supply constant power output irrespective of variations in load.

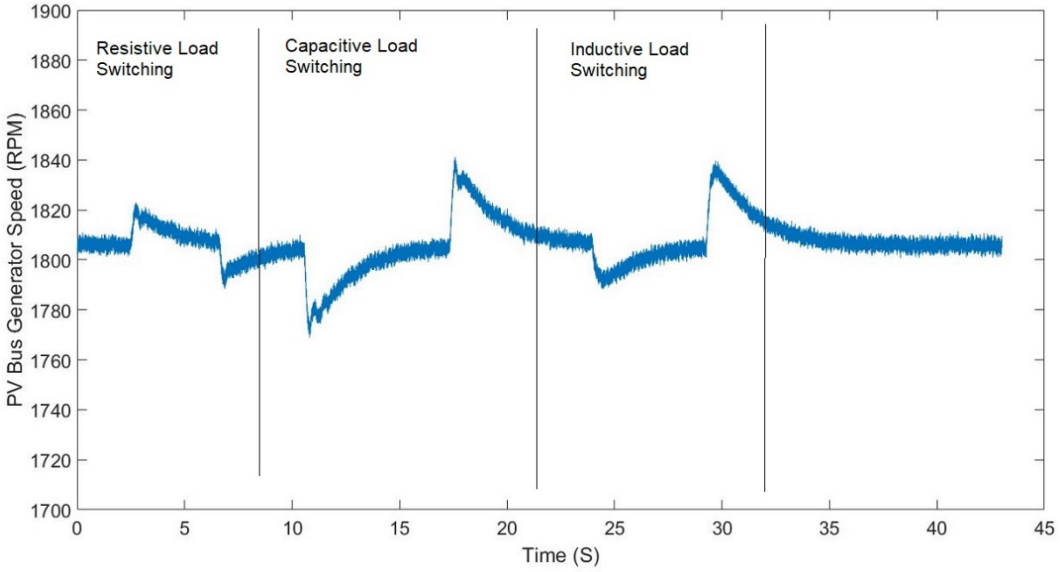

Figure 11 Generator Speed (PV Bus).

Figure 11 shows the speed of the PV bus generator which remained near 1800 rpm (except for a small bias in the measurement system). As expected, the speed varied during load switching, however returned to the normal speed within a few seconds. The speed of the slack bus generator was maintained constant by the dynamometer controller.

Overall, the baseline experimental data clearly demonstrates that the controllers for both the slack bus and the PV bus generators were operating as expected. The gains of the PI controller were acceptable to maintain the terminal voltage of the two generators as the nominal value of 75V. Next, we investigate the effects of cyberattacks on the PV bus generator control system.

3.2 Denial-of-Service Attack

This section presents experimental results of a (simulated) DoS attack on the PV bus generator excitation control system. Denial-of-service attack usually causes congestion in the network causing data packet drops, which affects the feedback control system. In this experiment, DoS attack was simulated at the software level; because of network security issues, an institutional permission was not feasible to allow actual DoS attacks on the excitation system. Data packets in

transition from the sensor to the controller were dropped according to a Bernoulli process; the packet dropout probability was a variable parameter for experimentation. This research utilizes the idea behind the UDP protocol for data transmission so that the simulated lost data packet is not retransmitted. Instead it was assumed that the controller holds the last successfully received sensor data and uses it to replace the lost packet. Figures 13-16 show the response of the three-bus system due to five different values of packet drop probabilities of Bernoulli packet drops of PV bus generator control loop.

For each packet drop probability β, the PQ bus loads were switched sequentially, first switching ON/OFF of a resistive load, then an inductive load followed by a capacitive load. As expected, switching of a resistive load causes a drop in load bus voltage, an inductive load causes a larger drop, and capacitive load causes an increase of voltage as shown in Figure 12. Note also that the slack bus voltage (middle window) and the PV bus voltage (top window) are held relative constant by the excitation system controller except for short time transients. The top window of Figure 12 shows the effects of packet drop on the PV bus voltage; the PV bus voltage becomes noisier with increasing levels of packet drop. Overall, the system remained stable for packet drop probabilities below a certain threshold[13].

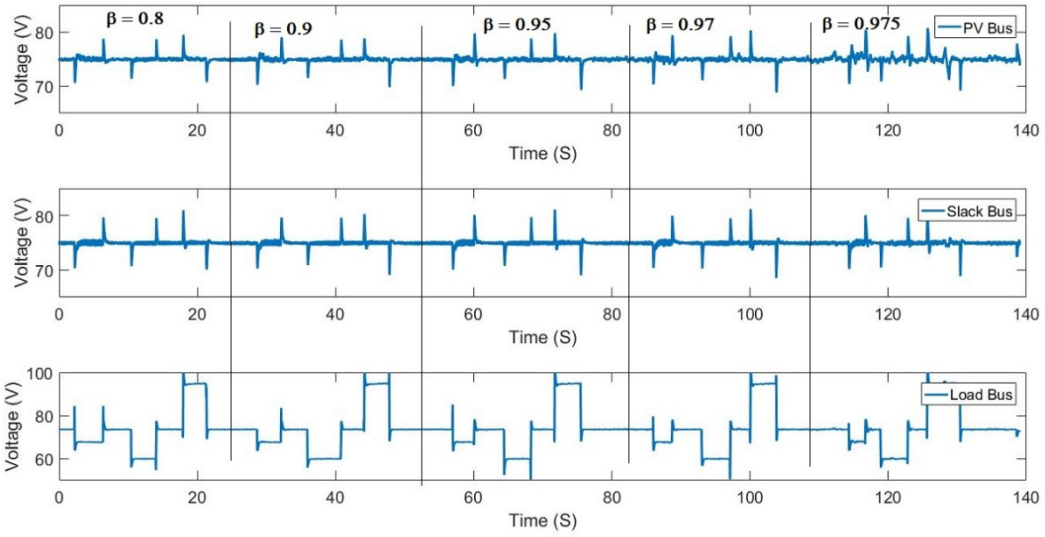

Figure 12 Bus Voltages (DoS Attack on PV bus generator).

Figure 13 shows the corresponding current injections at the various buses. The load bus current varies with load as seen from the bottom window of Figure 13. Clearly current injection at the PV bus (top window) is expected to remain constant since this generator supplies a constant power; transient variations are however observed during load switching. The slack bus generator supplies additional current as the load changes as shown in the middle window. Figure 14 shows the duty cycle ratio for different values of packet drop probability, which also shows increased sharp variations in duty ratio when the packet drop probability if high.

Variations in PV bus generator current also imply an imbalance between its prime mover input and electrical output which sets the generator into oscillations. This can be observed in Figure 15. Because of fast sampling rate of the system, overall the system remained stable even when the packet drop probability was 0.975, which depends on the sampling time of the controller.

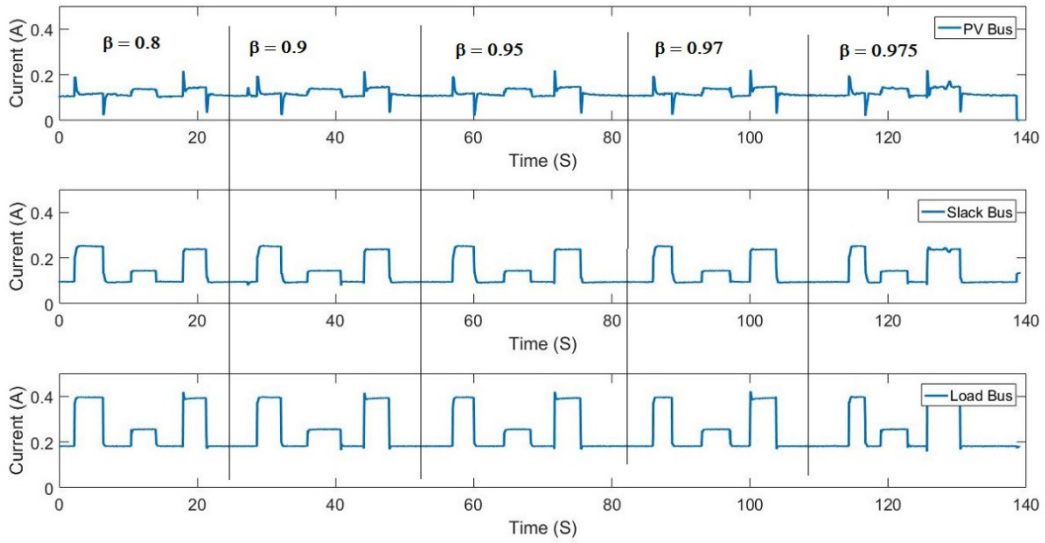

Figure 13 Bus Currents (DoS Attack on PV Bus Generator).

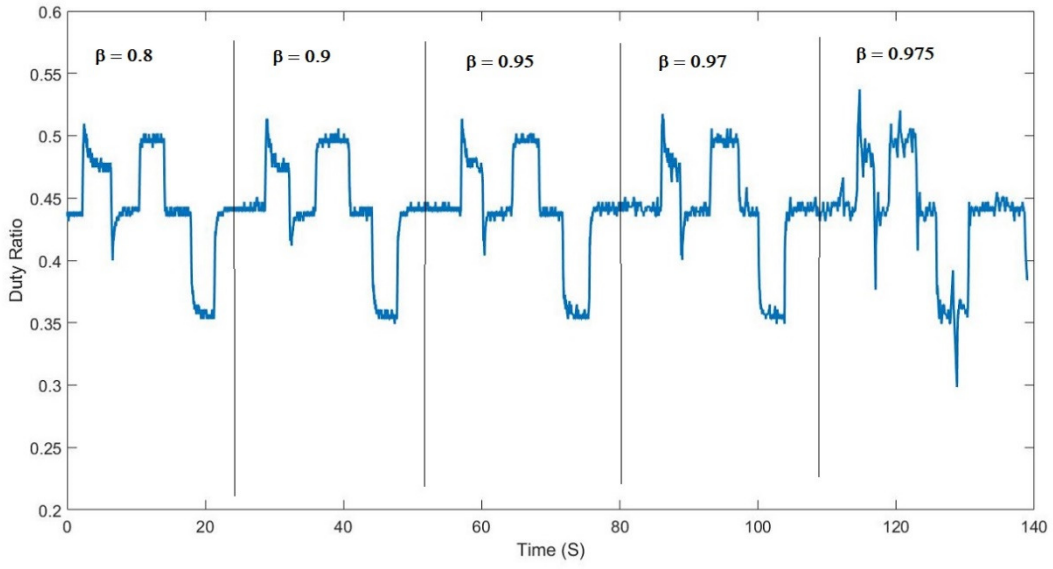

Figure 14 Duty Cycle Ratio (DoS Attack).

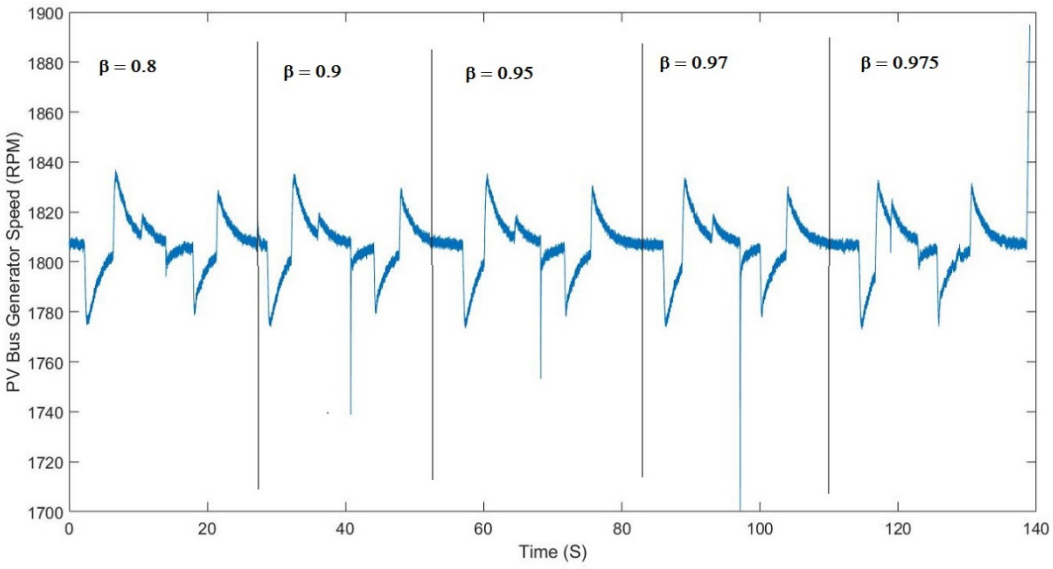

Figure 15 Generator Speed (PV Bus) (DoS Attack).

4.0 Classroom Demonstration and Student Feedback

A laboratory demonstration was performed before an audience of undergraduate students to determine the effectiveness of the platform as a teaching tool for power systems. An email announcement was sent to the ECE undergraduate student listserv about the date and time of the laboratory demonstration. The focus of the demonstration was to explain the how to synchronize generators, show fluctuations in the grid voltage due to various loads, and to perform a DoS attack to give the students a real-world view of the potential dangers of cyberattacks. To gauge the students' experience to the experimental demonstration, a multiple-choice questionnaire survey was conducted at the end of the demonstration.

The survey questionnaire and the students' responses are aggregated in Table 1. A total of 23 students attended the experimental demonstration and participated in the survey. Most of these students were juniors or seniors in Electrical and Computer Engineering, and many have taken at least one course related to power systems, however their academic preparation in the field as is considered as 'poor'. On the question on grid synchronization and loading, the students' response on understanding from the demonstration was about 50% 'Very Good' or 'Excellent'. On cyberattack on the grid, over 70% students ranked their understanding of the effects of cyberattack as 'Very Good' or 'Excellent'.

Table I Survey Questionnaire and Results

Questions	Answers					
I am a:	Freshman	Sophomore	Junior	Senior		
	1	1	8	13		
I have taken or currently taking at least one course in power:	yes			no		
	15			8		
I rank my knowledge of the power grid as:	Excellent	Very Good	Good	Poor	No Background	
	0	2	8	7	6	
I rank my knowledge of cyberattacks on the power grid as:	Excellent	Very Good	Good	Poor	No Background	
	0	1	4	9	9	
This experiment helped me understand generator synchronization:	Excellent	Very Good	Good	Poor	Didn't learn anything	**Total: Very Good or Excellent**
	7	6	10	0	0	56%
This experiment helped me understand how generators share loads in real time:	Excellent	Very Good	Good	Poor	Didn't learn anything	
	7	4	11	1	0	48%
This experiment helped me understand how grid voltages change as loads change from inductive to capacitive to resistive:	Excellent	Very Good	Good	Poor	Didn't learn anything	
	5	6	10	2	0	48%
This experiment helped me understand vulnerability of the power grid due to cyberattacks:	Excellent	Very Good	Good	Poor	Didn't learn anything	
	8	9	5	1	0	74%
This experiment helped me understand sequence of changes that might happen in the powergrid following a cyberattack:	Excellent	Very Good	Good	Poor	Didn't learn anything	
	5	11	7	0	0	70%

Overall, the demonstration was a fruitful endeavor as most of the students appeared to be truly interested in the subject matter and learned more about the power grid.

5.0 Conclusions

In this paper, we have presented a novel development of an HIL experimental platform for observing and evaluating cyberattacks on a real physical microgrid. We have provided an in-depth description of the experimental setup along with appropriate experimental results for normal operation and under DoS attacks. From an educational perspective, this experimental setup clearly shows how generators in a multi-bus system interact with changes in load condition. Denial-of-service attacks were launched on the defenseless system to prove the functionality of the controller and the ability to successfully maintain stability of the system under cyberattacks. The results demonstrate the impacts of cyberattacks on the microgrid and its stability. The platform can be used in senior level courses on power systems as a laboratory demonstration tool to show the impacts of cyberattacks, albeit simulated, on a real physical microgrid. Once fully developed, the platform can be used to evaluate cyber countermeasures capable of defending or preventing harm to the power grid.

6. Acknowledgement

This research was supported in part by grants from the National Science Foundation CNS-1446574, CNS-1446570, and CNS-1446621 and by the Office of Naval Research grant N00014-15-1-2922.

7.0 References

[1] E. J. Markey and Henry A. Waxman, "Electric Grid Vulnerability: Industry Responses Reveal Security Gaps", U.S. House of Representatives, Washington, DC, 2013.

[2] B. Wingfield, "Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months". Online at http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html, 2012.

[3] R. Rantala, "Cybercrimes Against Businesses", *Bureau of Justice Statistics*, 2008.

[4] S. Baker, S. Waterman and G. Ivanov, "In the Crossfire: Critical Infrastructure in the Age of Cyber War", McAfee, Santa Clara, California, 2009.

[5] A. Lipovsky and A. Cherepanov, "BlackEnergy Trojan strikes again: Attacks Ukrainian electric power industry", Online at http//www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry, 2016.

[6] Wall Street Journal, "U.S. Risks National Blackout from Small-Scale Attack", 2014.

[7] GAO (General Accounting Office), "Critical Infrastructure Protection: Challenges in Securing Control Systems", Online at http://www.gao.gov/new.items/d04140t.pdf, 2003.

[8] R. Nicholson, "Critical Infrastructure Cybersecurity: Survey Findings and Analysis", *Energy Insights*, 2008.

[9] L. Tinnel, O. Saydjari and D. Farrell, "Cyberwar strategy and tactics: An analysis of cyber goals, strategies, tactics and techniques", *Proceedings of the IEEE SMC Workshop on Information Assurance*, pp. 228-234, 2002.

[10] U.S. Government Accountability Office, "Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities and Remaining Challenges", *Report No. GAO-05-327*, Washington, DC, 2005.

[11] T.R. McJunkin, C. Rieger, B.K. Johnson, "Interdisciplinary Education through Edu-tainment: Electric Grid Resilient Control Systems Course", *ASEE Annual Conference and Exposition,* Seattle, Washington, 2015.

[12] M. Zeller, "Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator?", *proceedings of the 37th Annual Western Protective Relay Conference*, Spokane, WA, 2010.

[13] A. Rege, Frank Ferrese, Saroj Biswas, and Li Bai, "Adversary Dynamics and Smart Grid Security: A Multiagent System Approach", *7th International Symposium on Resilient Control Systems (ISRCS2014*), August 18-21, 2014, Denver, CO.

[14] J. Kollmer, Robert Irwin, Saroj Biswas, Walid Saad, Arif Sarwat, Li Bai, "Development of an Experimental Platform for Analysis of Cyberattacks on Power Grid", *ASEE Annual Conference and Exposition, Columbus*, OH, June 25-28, 2017.

[15] S. Biswas and Arif Sarwat, "Vulnerabilities in Two-Area Automatic Generation Control Systems under Cyberattacks," *International Symposium on Resilient Control Systems (ISRCS2016)*, Chicago, August 16-18, 2016.

[16] M. Sloderbeck, C. Edrington, and M. Steurer, "Hardware-in-the-Loop Experiments with a Simulated Electric Ship Power System utilizing a 5 MW Variable Voltage Source Converter Amplifier", *IEEE International Conference on Electric Machines and Drives Conference, IEMDC '09,* May 2009.

[17] Van H. Nguyen, Y. Besanger, Q. Tuan, C. Boudinnet, and T.L. Nguyen, "Using Power-Hardware-in-Loop Experiments together with Co-Simulation for the Holistic Validation of Cyber-Physical Energy Systems", *IEEE PES Innovative Smart Grid Technologies, ISGT* Europe, 2017

[18] R. Brandi, Mihai Calin, and T. Degner, "Power Hardware-in-the-Loop Setup for Power System Stability Analysis", *24th International Conference on Electricity Distribution*, Glasgow, June, 2017.

[19] X. Wu, S. Lentijo, and A. Monti, "A Novel Interface for Power-Hardware-in-the-Loop Simulation", *IEEE Workshop on Computers in Power Electronics*, Aug, 2004.

[20] G. F. Lauss, M. Omar Faruque, K. Schoder, C. Dufour, A. Viehweider, and J. Langston, "Characteristics and Design of Power Hardware-in-the-Loop Simulations for Electrical Power Systems", *IEEE Transactions on Industrial Electronics*, Vol. 63, pp. 406-417, 2016.

[21] S-T Cha, P. Kwon, Q. Wu, A. Nielson, and J. Ostergraad, "Real-Time Hardware-in-the-Loop Testing for Digital Controllers", *Proc. IEEE PES Asia-Pacific Power and Energy Engineering Conference*, 2012.

[22] M. Almas and L. Vanfretti, "Experimental Performance Assessment of a Generator Excitation Control System using Real-Time Hardware-in-the-Loop Simulation", *Proc. 40th Annual Conference of IEEE Industrial Electronics Society, IECON201*4, Nov 2014.

[23] J. Jung, "Power hardware-in-the-loop simulation (PHILS) of photovoltaic power generation using real-time simulation techniques and power interfaces," *J. Power Sour.*, Vol. 285, No. 7/1, pp. 137–145, 2015.

[24] Y. Zhou, J. Lin, Y. Song, Y. Cai, and H. Liu, "A power hardware-in-loop based testing bed for auxiliary active power control of wind power plants," *Electr. Power Syst. Res.*, Vol. 124, No. 7, pp. 10–17, 2015.

[25] M. Milosevic, P. Prempraneerach, J.L. Kirtley, G. Karniadakis, C. Chryssostomidis, "An end-to-end simulator for the all-electric ship MVDC integrated power system," in *Proceedings of the Grand Challenges in Modeling and Simulation (GCMS10)*, Ottawa, Canada, 2010.

[26] S. Paran, T. V. Vu, F. Franco, and C. S. Edrington, "Evaluation of the Interface Accuracy for Power Hardware-in-the-Loop Experiments", *Journal of Electric Power Components and Systems*, Vol 45, pp. 763-773, 2017.

[27] A. Sanjab and W. Saad, "Data Injection Attacks on Smart Grids with Multiple Adversaries: A Game-Theoretic Perspective," IEEE Transactions on Smart Grid, Special Issue on Theory of Complex Systems with Applications to Smart Grid Operations, vol. 7, no. 4, pp. 2038-2049, July 2016.