ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION

Paper ID #40565

# Teaching Critical Infrastructure Cyber Security to Undergraduate Students using Real-Time Hardware-in-the-Loop Cyber-Power Testbed

**Mohammed Mustafa Hussain**
**Dr. Sagnik Basumallik, West Virginia University**

Sagnik Basumallik is with the Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV 13244 USA. Sagnik's research interests include power systems cybersecurity, operations, and optimization. In the past, he has worked in a different capacity at the University of Colorado-Boulder, Brookhaven National Laboratory, Independent System Operator, New England, Siemens India, Indian Institute of Technology, Mumbai, and Durgapur Projects Limited.

**Dr. Anurag K. Srivastava, West Virginia University**

Anurag K. Srivastava is a Raymond J. Lane Professor and Chairperson of the Computer Science and Electrical Engineering Department at the West Virginia University. He is also an adjunct professor at the Washington State University and senior scientist at the Pacific Northwest National Lab. He received his Ph.D. degree in electrical engineering from the Illinois Institute of Technology in 2005. His research interest includes data-driven algorithms for resilient power system operation and control and engineering education. In past years, he has worked in a different capacity at the Réseau de transport d´électricité in France; RWTH Aachen University in Germany; PEAK Reliability Coordinator, Idaho National Laboratory, PJM Interconnection, Schweitzer Engineering Lab (SEL), GE Grid Solutions, Massachusetts Institute of Technology and Mississippi State University in USA; Indian Institute of Technology Kanpur in India; as well as at Asian Institute of Technology in Thailand. He is serving as chair of the IEEE Power & Energy Society's (PES) PEEC committee, co-chair of the microgrid working group, vice-chair of power system operation SC, chair of PES voltage stability working group, chair of PES synchrophasors applications working group, co-chair of distributed optimization application in power grid, vice-chair of tools for power grid resilience TF, and member of CIGRE C4C2-58 Voltage Stability, C4.47/ C2.25 Resilience WG. Dr. Srivastava is serving or served as an editor of the IEEE Transactions on Smart Grid, IEEE Transactions on Power Systems, IEEE Transactions on Industry Applications, and Elsevier Sustainable Computing. He is an IEEE Fellow and the author of more than 300 technical publications including a book on power system security and 4 patents.

**Dr. Mohamed Hefeida, West Virginia University**

# Teaching Cyber Security of Critical Infrastructure to Undergraduate Students using Real-Time Hardware-in-the-Loop Cyber-Power Testbed

Hussain M Mustafa, Sagnik Basumallik, Anurag K Srivastava, Mohamed Hefeida
Lane Department of Computer Science and Electrical Engineering
Benjamin M. Statler College of Engineering and Mineral Resources
West Virginia University, Morgantown, WV

## Abstract

This paper discusses efforts to develop a real-time cyber-physical security testbed for the hands-on training and education of undergraduate students. The developed cybersecurity testbed has been used for an undergraduate course and senior capstone project. The testbed helps students to specifically learn about cyber threats against critical electricity infrastructures and develop appropriate defense mechanisms by utilizing MITRE ATT&CK adversary emulation techniques, NERC CIP compliance, and NIST Cybersecurity Framework. To mimic a realistic power substation network, we have developed a three-tier architecture through a mix of simulation, emulation, and actual hardware implementation, consisting of the power system substation, communication network, and monitoring/control center layer. The substation layer enables students to integrate components including generators, electric bus bars, switches, transformers, and distributed energy resources such as solar, wind, and large-scale battery. Here, multiple industry-graded sensors and actuators have been integrated to capture real-time voltage and current measurements and enable remote control and protection schemes. These help students to get acquainted with different industrial automation standards and protocols such as IEC 61850, DNP3, and Modbus in critical infrastructure operational technology (OT). The communication network layer, consisting of a combination of software-defined networking and traditional networking, allows the students to learn state-of-the-art network technology paradigms, features, and how they are involved in exchanging end-to-end critical infrastructure system data. At the monitoring/control center layer, the students are able to capture and visualize the cyber and power data from multiple sources and develop machine learning-based anomaly detection, classification, and localization tools to improve cyber power security and cyber-resiliency. Industry-standard security information and event management tools such as Splunk and intrusion detection systems are used to train students to detect, defend and analyze coordinated cyber attacks. The hardware-in-the-loop learning ecosystem lets the students perform red-team and blue-team exercises for power systems following cybersecurity standards, guidelines, and related frameworks. As an outcome, the students develop an understanding of cyber security concepts such as digital forensics, incident response, and reverse engineering related

to the power grid, and are able to design steps to keep the grid infrastructure secured. Overall, our approach advances the cybersecurity profession through hands-on training and helps develop a robust talent pipeline to meet the increasing demand for cybersecurity jobs that affect national security.

# 1 Introduction

The integration of advanced communication infrastructure and information technology into the traditional electric power grid has given rise to a resilient and reliable smart grid architecture. However, this complex convergence of advanced technologies has brought several cyber-physical challenges, which include events like the Ukraine power grid cyber attacks[1], Texas blackouts[2], and physical sabotage of North Carolina substations[3]. The extreme economic and societal impacts of such catastrophic events call for a growing need for future workforce development capable of handling the multiplex inter-dependencies of the cyber and the power system. The White House has recently identified approximately 700,000 cybersecurity open positions at the National Cyber Workforce and Education Summit and has prioritized the need to invest in cyber training, education, and skill-based pathways to tackle the national security challenge[4]. With the vision of creating a new-generation workforce trained with relevant cyber skills for the critical power infrastructure, West Virginia University has set up the **S**mart **G**rid **RE**siliency and **A**nalytics **L**ab (SG-REAL). The SG-REAL provides undergraduate students with a state-of-the-art smart grid cybersecurity testbed platform and a **G**rid **O**peration **L**ab (GO-Lab) that is integrated into coursework curriculum and extensively used to conduct advanced classroom research and experiments on cyber-physical resiliency, security, stability, and operator training. This real-time multi-vendor hardware-in-the-loop testbed is integrated into the newly introduced CPE 435 - Computer Incident Response course at the WVU and provides the students with a wide range of open-source and industry-grade software and hardware for analyzing critical infrastructure incident response, forensics, and computer security for smart grid systems.

Integrating the cyber-physical SG-REAL testbed into the curriculum meets the need for interdisciplinary cyber and power training courses and provides a strategic hands-on program for the students to understand smart grid components, working principles, and vulnerabilities. It allows students to carry out offensive vs defensive security training based on the MITRE ATT&CK Framework framework and makes them familiar with how to practice the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) compliance for cyber security using real-time SG-REAL environment. Incorporating the test-bed platform early on in the coursework develops not only the technical but also the interpersonal skills of the students - it allows them to comprehend concepts of shared responsibility where the actions of cyber experts directly impact the power grid and vice-versa. Ultimately, this aids in training and preparing undergraduate students on how to defend key power grid infrastructure against sophisticated cyber-physical attacks as the new-generation system operators, deemed extremely valuable for national security.

The rest of the paper is organized as follows. Section 2 provides a literature review of existing cybersecurity teaching efforts. Section 3 & 4 gives an overview of the industry-grade cyber-physical power system testbed and its integration into cybersecurity teaching. Section 5 highlights various teaching experiences while Section 6 focuses on student learning outcomes, with conclusions

presented in Section 7.

## 2 Related Work on Cyber-Power Security Teaching

Previous efforts in developing the 'Cyber infrastructure for the smart grid' course at the undergraduate level by one of the authors of this paper have been extremely successful in combined teaching of power systems, communication, computation and data management, cybersecurity, and cryptography, as well as creating an industry-based case study learning opportunity[5,6]. A related effort was made to develop an industry-grade cyber–physical distribution management system that integrated remote terminal units, smart meters, and solar arrays and enabled students to develop attack detection algorithms and study impact analysis[7]. An interactive cybersecurity learning system was developed focusing on cyber attack and defense where the students were provided with their own virtualized environments[8]. Simulated laboratory platforms were used to develop cyber security modules focusing on the Industrial control systems vulnerability and defense methodologies in[9]. An introductory course design about cyber-physical systems focused on the different theoretical concepts[10]. The cyber security lab was renovated from an infrastructure perspective, and integration of a learning management system and usage of LabVIEW-based engineering platforms to perform real-life emulated experiments [11,12].

## 3 Real-Time Critical Infrastructure Hardware-in-the-Loop (HIL) Cybersecurity Testbed

Critical infrastructure refers to a system whose assets, networks, and services are so essential that minimum unavailability of their services can result in a debilitating impact on the national economy, public health, and our day-to-day activities. According to the cybersecurity & infrastructure security agency (CISA)[13], there are 16 sectors that are considered to be critical infrastructure, and the energy sector is one of the most important. Moreover, the US Presidential Policy Directive 21[14] has identified the energy sector as 'uniquely critical' as it enables the functioning of other dependent critical infrastructures such as communication, transport, water, and gas. The stable supply of electricity can be affected for many reasons, which can be broadly classified as,

1. Physical and natural events that include natural events such as hurricanes, snow storms, and wildfires[2],[15], or physical damage such as terrorist acts[3].
2. Cyber attacks against smart grid automation, control, monitoring infrastructure, and communication network failure[16,17].

This section describes the SG-REAL state-of-the-art smart grid cybersecurity testbed and a Grid Operation (GO) testbed that is integrated with undergraduate teaching which enables students to conduct research on multiple fronts of grid resiliency, security, stability, and operator training.

## 3.1 Overview of the Testbed

Our testbed provides a platform for developing, testing, and validating different cybersecurity strategies and tools that improve grid resiliency under cyberattacks. The real-time digital simulator (RTDS) simulates the underlying physical power system in real-time and interfaces with the external hardware through software applications embedded. The platform consists of state-of-the-art sensors and actuators providing grid automation and control capabilities. Communication network devices comprise both Software-Defined Networking (SDN) and traditional networking. For emulating different network scenarios involving Wi-Fi, Wimax, and optical fiber, various network simulation tools are available. A wide range of open-source and industry-grade software is utilized to generate, store, and analyze high-fidelity cyber-power data. These features together make the testbed an advanced real-time multi-vendor hardware-in-the-loop industry-graded platform. Detail of various testbed components and their functionalities, and how they relate to student learning of critical infrastructure cyber security are discussed next.

## 3.2 Components and Functionality

### 3.2.1 Real-Time Digital Simulator (RTDS)

The RTDS simulator performs a real-time electromagnetic transient simulation of the power system[18]. The parallel processing hardware, NovaCor, is custom developed to run simulations in real-time over a wide range of frequencies with a timestamp of 25-50 microseconds. Various I/O cards provide additional capabilities to demonstrate multiple cyber-power use cases for power system protection, automation, and monitoring. These include,

1. Analogue input and output cards: The Giga-Transceiver Analogue Output (GTAO) and Input (GTAI) cards can be connected to external equipment directly at $\pm 10$ V peak. In our case, it is connected to SEL 401 Merging Unit (MU) which is a remote data acquisition device.
2. Digital input and output cards: The Giga-Transceiver Digital Output (GTDO) and Input (GTDI) cards connect with the external devices between +5V to +30V dc. It is used to receive relay trip signals from MUs.
3. Ethernet-based communication cards: GTNETx2 is an ethernet-based communication card that interfaces directly with external devices to stream data via communication protocols such as IEC 61850, MODBUS, DNP3, and C37.118 for different smart grid applications.

Together, these features offer undergraduate students an overview of how the actual power system operates and interacts with smart devices, and offer opportunities for classroom integration and undergraduate research.

### 3.2.2 Sensors and Actuators: Substation Automation, Protection, and Control

Smart sensors and actuators drive the advanced power system automation, protection, and control technology. While it is highly imperative that the students learn about the sensors and actuators, however, due to privacy and security concerns, such knowledge transfer is often not directly available hands-on in power utilities. SG-REAL provides an opportunity for undergraduate students in WVU to have hands-on exposure to various industry-graded sensors. These include a variety

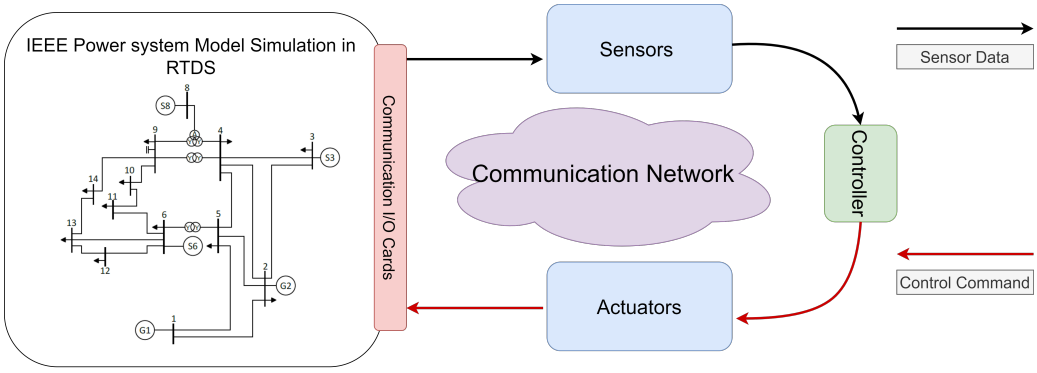


Figure 1: Sensors and actuators communicating with RTDS via communication network

of Schweitzer Engineering Laboratories (SEL) relays/Intelligent Electronic Devices (IEDs), MU, Global Positioning System (GPS) clock, and Real-time Automation and Controller (RTAC). A brief overview of various components is provided below.

1. SEL IED and MU: SG-REAL hosts multiple SEL 451, SEL 421, and SEL 401 devices connected via communication networks. They enable automation, protection, and control of substations through the exchange of time-critical data using communication protocols such as IEC 61850 (GOOSE, SV, and MMS), Supervisory Control and Data Acquisition (SCADA) protocols such as MODBUS and DNP3, and synchrophasor protocol such as C37.118. Generally, RTDS simulates the power system and sends data to SEL 401 MU or SEL 451 IEDs through analog signal or SV protocol, and SEL IEDs and MU communicate via GOOSE for the operation of circuit breakers in the RTDS power system model. SEL 451s also work as Phasor Management Units (PMU), sending time-synchronized current and voltage phasor data at 30-60 samples per second via C37.118 to the control center Phasor Data Concentrator (PDC). These PMU data can be further used to provide state estimation and other power system downstream applications.

2. SEL Real-Time Automation and Controller (RTAC): The SEL 3350 RTAC works as SCADA by subscribing data from the SEL IEDs through DNP3/MODBUS and can control circuit breakers remotely. Additionally, it works as a PDC by subscribing C37.118 data from RTDS GTNETx2 software PMU or SEL 451 PMU, organizing and sending C37.118 data to desired applications.

Fig 1 shows sensors, actuators, and controllers communicate with RTDS using a communication network. The various SEL IEDs, RTAC, and MU provide students with an opportunity to understand protocol communication, how applications utilize these protocols to exchange data, and their subsequent usage. With hands-on experiments and class projects, the students are able to gain a deeper understanding of the various security risks associated with those protocols which can violate the grid data Confidentiality, Integrity, and Availability (CIA). Above all, familiarization with SEL and other industry-graded hardware devices provides students with a great advantage in the job market for critical power system cybersecurity.

### 3.2.3 Communication Network: Component, Technology, and Design

The communication network of the SG-REAL lab consists of multiple types of hardware devices and software tools. A brief overview of each component is given below.

1. Network hardware devices: The cybersecurity testbed is equipped with multi-vendor (i.e., SEL, CISCO, and Netgear) network switches and routers which are used to configure and design real-world network scenarios. An example work of NS3 network communication in the smart grid can be found in[19].

2. Software network emulation tools: Network emulation tools such as open-source Network Simulator 3.0 (NS3) and MININET emulate various network scenarios and extend the communication network scale by interfacing it with real devices such as sensors, actuators, or hardware network devices.

3. Software-Defined vs Traditional networking: SG-REAL has incorporated SDN, an emerging concept in networking that provides a good alternative choice for traditional networking approaches[20]. While SDN is more common in Information Technology (IT) networks, its usage in smart grid Operational Technology (OT) devices is yet to be widely adopted. SDN provides systems operators with the ability to programmatically set up the network, perform proactive traffic engineering, and control the network through a centralized control plane using a protocol called OpenFlow. Unlike traditional networking, SDN separates the control plane from the data plane, thereby reducing the overhead of each device and increasing manageability. SDN has proved to be a viable alternative for the smart grid OT networks considering the high-frequency data requirement of real-time applications to provide a quick situational awareness to network operators[21,22].

The hardware-in-the-Loop tested simulation platform provides the students with real-world hands-on experience in networking and data communication. Using the software network emulation tools, the students are able to emulate various technologies such as Wi-Fi, Wimax, Zigbee, Ethernet, and optical fiber. Additionally, they are able to create very large networks by emulating the traffic of real-world scenarios considering different service constraints such as bandwidth, jitter, and latency. Using a combination of real hardware, SEL 2740, and SEL SDN flow controller 5056, the students are able to create, and manage SDN flows and compare the performance of traditional networking using CISCO and Netgear devices with the SDN for smart grid communication requirements.

The industry-grade setup at SG-REAL provides students with additional opportunities for network vulnerability analysis customized for the cybersecurity and incident response course. Students are able to create scenarios that involve smart grid data exchange through various network protocols such as C37.118 (for streaming high-frequency voltage and current phasors), DNP3 (for traditional SCADA measurements), and IEC 61850 (for protection and automation). As a result, the students are able to understand normal vs anomalous operations of these protocols, allowing them to develop advanced vulnerability analysis algorithms and tools.

### 3.2.4 Cyber Security Information and Event Management (SIEM) and Data Storage

SG-REAL offers real-time cyber monitoring and event analysis tools that help users to track and log cyber data across all devices in the network. In addition, all cyber-power data obtained from

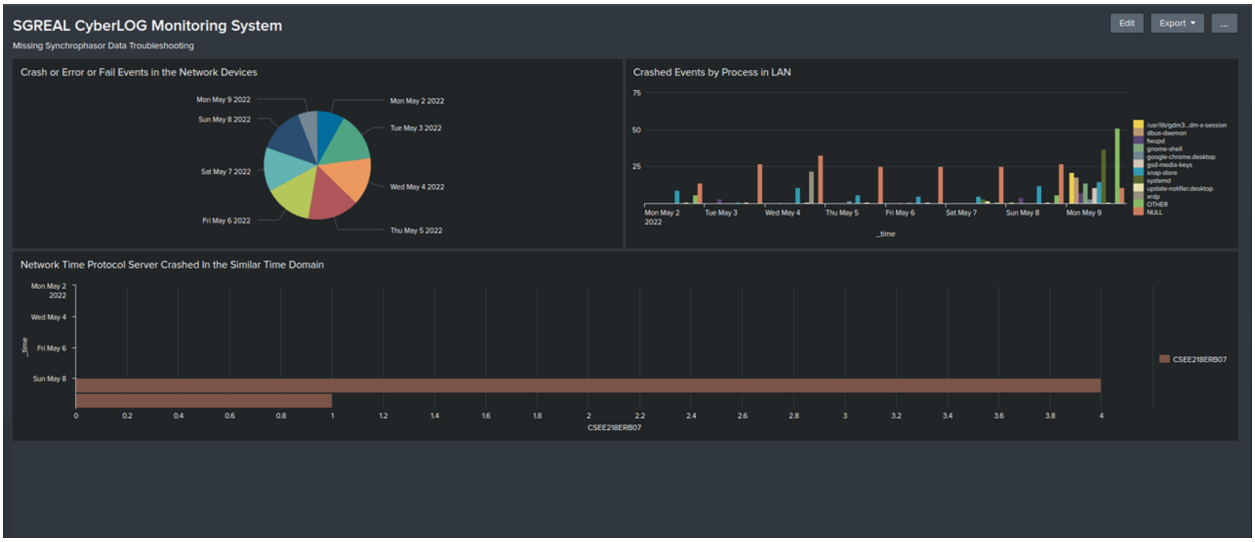


Figure 2: Using SIEM to monitor specific events within network devices

this platform can be stored either locally or in the cloud. A brief overview is given below,

1. Cyber security information and management, intrusion detection system: For incident response and forensic analysis, a wide variety of cyber events and information is collected. SG-REAL platform uses a Security Information and Event Management (SIEM) tool called Splunk which ingests data from various sources such as sensor and actuators, system logs and network traffic from network devices, human-machine interfaces, databases, and other machine events based on user-defined rules. Additionally, an open-source intrusion detection system, SNORT, is interfaced with Splunk to provide alerts in cases of different cyber anomalies.

2. Data storage: The cybersecurity testbed is equipped with both local and cloud database storage systems to store the huge amount of data obtained from various physical devices such as RTDS, relays, and PMUs. For local storage, data is accumulated via PDCs and SCADA and stored in a local MySQL database. For cloud storage, the data is stored in a PingThings database[23].

Fig 2 shows how Splunk is used as SIEM to monitor crashed events within the network devices and root cause analysis for the specific events. The SIEM tool allows students to capture data from a wide range of assets at one centralized location, perform log and incidence monitoring, analyze data, and recognize threats in real-time, thereby providing opportunities to strengthen grid cybersecurity. A portion of the data stored in the cloud is made public so that it can be used by students and researchers from other universities to develop advanced tools for grid operations.

Fig 3 shows the entire testbed architecture in detail as described above.

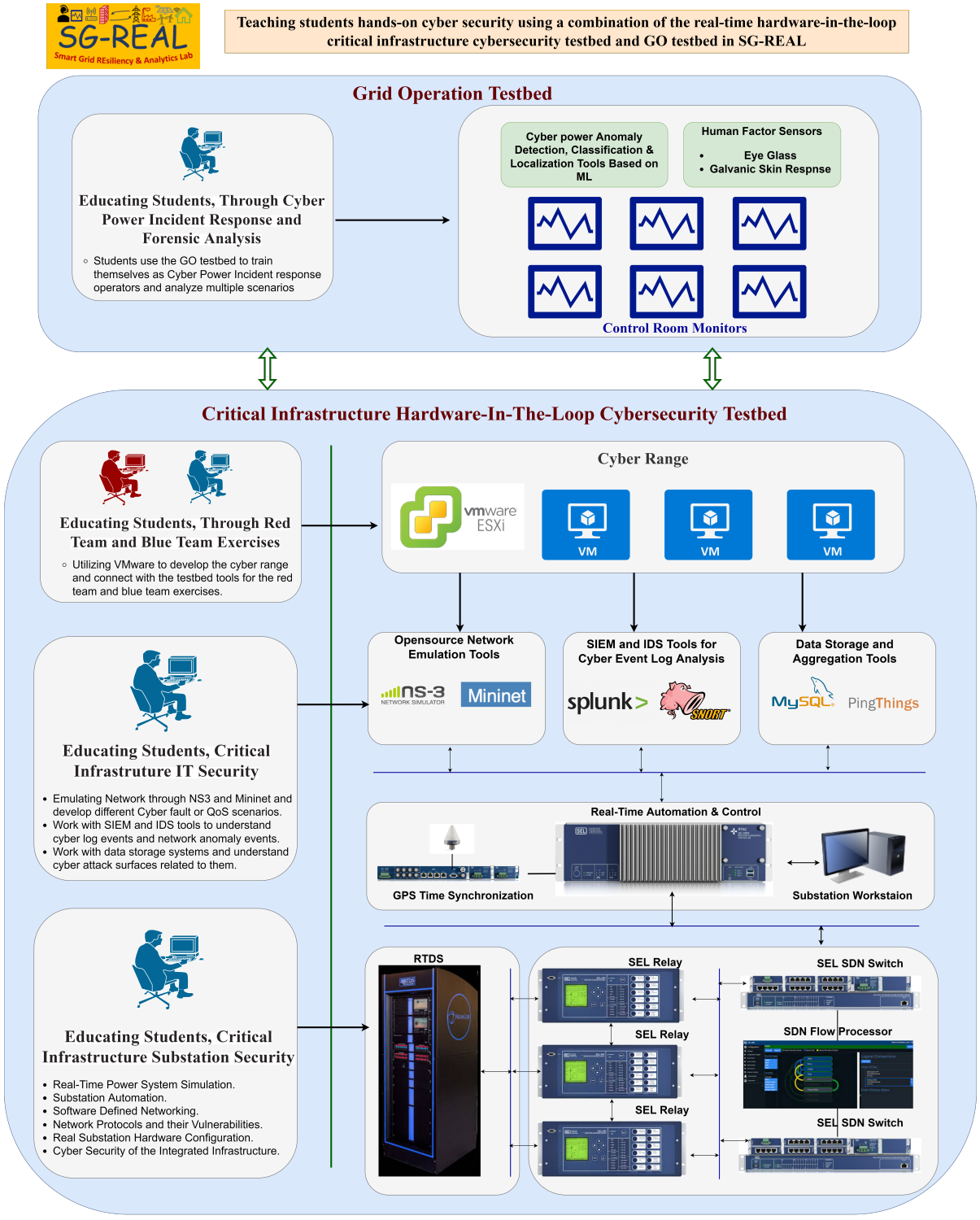


Figure 3: Interactive cybersecurity teaching using multiple components of the real-time hardware-in-the-loop critical infrastructure cybersecurity testbed and GO testbed in SG-REAL.

# 4 Grid Operations (GO) Testbed

In addition to the SG-REAL platform, West Virginia University hosts the Grid Operations (GO) testbed shown in Fig 3 that has the following components:

- Control room visualization: The visualization layer consists of multiple HMIs that feature dashboards from applications such as single-line diagrams, high-fidelity synchrophasor data, advanced tools, alarms, SDN, and cyber log monitoring.
- Advanced tools: Advanced tools such as CP-TRAM[24] quantify the resiliency of cyber-physical transmission systems and SyncAED[25] detect, classify, and locate events and anomalies through multiple base detectors using machine learning approaches.
- Human factor sensors: Eye-glass and Galvanic Skin Response (GSR) sensors are utilized for human factor studies pertaining to operator training.

These components together provide the students a holistic platform for advanced visualization and monitoring, as well as allows researchers to perform human performance analysis under extreme event and decision making.

# 5 Teaching Experience: Critical Infrastructure Cybersecurity

This section discusses several experiences in integrating the cyber-physical testbed into the academic curriculum of the Computer Incident Response course. As discussed previously, the hardware-in-the-loop testbed integrates into itself a large number of connected devices and numerous sensors generating enormous amounts of data that is continuously transferred over the network. This unprecedented amount of data generated, its criticality, the autonomy of devices generating the data, along with data analysis have invigorated the need for cybersecurity at every level of the network, from application to the physical layer. Despite the general idea of cybersecurity traditionally being part of computer science education, it has evolved into a multidisciplinary/meta-disciplinary subject[26]. Fig 3 summarizes the different aspects of cybersecurity teaching using the real-time critical infrastructure HIL cybersecurity testbed and GO lab in SG-REAL.

The Computer Incident Response course integrates critical grid infrastructure with computer system cyber security where the students understand the general working of the various power system and cyber system components, along with their vulnerabilities and cyber security framework, handling computer hardware, acquiring evidence in a computer forensics lab, online investigations and documentation, admissibility of evidence, network forensics and incident response, basic knowledge of important National Institute of Standards and Technology (NIST) guidelines and understand policies and associated controls to assist in safeguarding an organization. In addition to the technical and problem-solving skills, integration of this testbed has encouraged social skills among the students, which are deemed to be of utmost importance[27,28]. For example, the teamwork required in cybersecurity is often a result of a multi-function team, rather than a group software engineering activity that most educators implement in their classrooms[26]. This calls for relevant, multidisciplinary, multi-faceted projects that are designed with both technical and human skills in mind. Generic hands-on projects are more often implemented at the capstone level, which may be

insufficient to engrave these much-needed skills in students at an early stage in engineering education. This has been the feedback received by many educational institutions around the world from their industrial partners/advisory board members[29]. To improve the integration of these much-needed people skills, this course has incorporated a hands-on learning environment where students work on realistic cybersecurity challenges at a much earlier stage than the capstone project, which has been identified as one of the key factors setting this new course apart.

Having the SG-REAL testbed within the curriculum allows the students to make a stronger and more personal connection with real-world applications and critical scenarios. The impact of such a physical testbed is much more profound than currently available virtual environments. Despite having practical lab assignments that covered several essential areas of cybersecurity, including stenography, and cryptography, among others, the overwhelmingly positive response after a single visit to the cyber-security hardware laboratory was a turning point for many students. While the lab visit was not mandatory, yet was very well attended with over 90% of the class actively participating. The effect this engagement with a testbed had on the students was tremendous as most of them were able to experience the importance and criticality of what they have been learning and how they can apply it. The exact same concepts and assignments immediately became more interesting after seeing a real-life scenario of a power system. Being exposed to the various power grid components and related issues, working with the SG-REAL gave the students a deeper sense of importance, value, and need for their skills, which positively reflected on their engagement in the classroom. For example, students performed significantly well on one very closely related assignment that involved multiple attack steps between the two machines, including password cracking and Ping flooding attacks. This was evident from the number of submissions and overall grades received. In addition, the instructors of this course have witnessed emotional constructs in engineering education through course evaluation, which have been deemed important[30].

In addition to coursework and project integration of the SG-REAL, the instructors have witnessed an overwhelming response by including competitions to motivate students, using real-world problem-solving scenarios. A particular example of this includes the National Cyber League competition (NCL) in the class, which had a tremendously positive effect. Not only did it serve as a vehicle for training students and gaining needed skills, but it also allowed them to have a realistic evaluation of their skills among 7500 students from over 500 other institutions. Being placed top 10% in NCL was definitely rewarding for both students and mentors, and this effort was recognized by the office of the West Virginia State Governor. It was realized that exposing the students to a cyber-physical testbed early on in the class motivated them to take the competition more seriously, after understanding the extent of the damage that may result from a single password compromise.

Some of the student feedback include,

1. "*The powerpoints and book helped me out a lot, but I think I learned the best with labs and NCL*"
2. "*NCL should be stressed more in this course*"
3. "*Definitely both NCL and group project helped me learn a lot*"

# 6 Student Learning Outcomes using the Cyber-Power Testbed

## 6.1 Class Assignments

As discussed earlier, one of the objectives of the SG-REAL testbed is to detect, identify and provide root cause analysis of various cyber power incidents related to the electric grid. The various class assignments reflect how closely they can be implemented on the SG-REAL testbed. To this end, the students have learned to,

1. Navigate basic networking commands and understand basic level network activities monitoring, basic networking command practice, understand packet loss, packet drop, transmission failure,
2. Use of "Wireshark" as a Packet Capturing Tool to decode packet information, capture packets belonging to specific domains, and obtain IP addresses of websites,
3. Installation of Virtual Machine (VM) and virtual operating systems, and setup of the virtual cyber lab and private network,
4. Using Kali Linux to initiate cyber attacks, perform network penetration, checking vulnerabilities; using Ubuntu Operating System (OS) as a victim machine of all the simulated attacks/penetration testbed; using snort IDS as intrusion detection system on the Ubuntu OS to prevent cyber intrusion of Kali Linux.

Given the experience with the classroom projects, the students embarked upon the final project that required them to investigate a case of network breaching that has been manually configured from inside of the network. The students were able to monitor log files and captured packets from various computers to find the desired IP. Finally, an incidence response report was submitted following NIST frameworks/standards.

## 6.2 Cyber Range for Red team and Blue team exercises

A VMware ESXi standalone bare metal hypervisor is dedicated to developing virtualized on-demand cyber range environments. This cyber range includes virtual hosts connected with the HIL cyber security testbed components allowing students to perform red team exercises implementing cyber attack chains following MITRE ATT&CK ICS tactics and techniques, and blue team exercises through the utilization and understanding of the tools, devices, and protocols mentioned earlier.

## 6.3 Senior Design Capstone Project

The cyber security testbed was used for a senior design project where the students utilized RTDS and different SEL relays to develop a cyber security use case scenario. The project consisted of three main layers: the substation layer, the network layer, and the control layer. The substation layer runs the power system inside RTDS. The network layer takes the GOOSE packets from the substation layer and relays them to the control layer. The data returned is routed to the network layer where the switch can route the packets to the router and the router passes them to the control

layer switch. The control layer filters these packets and collects data to store in the database, which is subsequently used for visualization. Scapy is utilized to pass the packets into a Python script that will interact with the controller, database, and detection model. This is also where one can visualize the actual packets that are being sent through. The whole cyber power system is set up on an IEEE 13-node benchmark with an OpenDaylight network controller. With this setup, the students identified and analyzed the benefits of SDN in smart grid OT cyber security. Another goal was to develop cyber attacks in the grid and generate the data comprising both attack and normal scenarios and finally use those data to identify anomalies in the network. The specific tasks for setting up the project involved,

1. Creating the Virtual SDN Network and adding network controller in MININET.
2. Develop IEC 61850-based communication using GOOSE.
3. Connect external devices to Communicate with SEL Relays.
4. Cyber attack design and implementation.

Some of the outcomes of the senior design project implemented on the SG-REAL cyber-physical testbed include,

1. Understanding MITRE ATT&CK framework: As per the real system, the students were able to develop MITRE ATT&CK adversary emulation for industrial control systems and develop techniques for cyber attack chains. The state-of-the-art resources in the lab provided the students with multiple opportunities to see and analyze the impacts of cyber attacks in utility substations and understand the vulnerability across multiple access points, network protocols, and the overall network.
2. Understanding NERC CIP compliance: The NERC CIP standards have been developed to protect the power system against a wide range of cybersecurity aspects, and cover physical security, network security, incident response plans, configuration management, and vulnerability assessments. It has now become mandatory for energy utilities to comply with these standards against the growing threats. At SG-REAL, the students are able to practice these CIP standards on real systems, learn how to generate data, and report it accordingly in times of an incident.

# 7 Summary

Cyber-physical security-related incidents against critical power grid infrastructures are becoming more and more significant. Understanding the diverse security aspects, and reducing the overall vulnerability of the grid still remains an open issue. This work aims to fill the gap by introducing a real hardware-in-the-loop cyber-physical testbed at West Virginia University into the undergraduate course curriculum of computer security incidence response. Hands-on training allowed the students to study a variety of topics related to power systems, grid security, resilience, how the power system actually functions and interacts with smart devices, network vulnerability analysis, and security threats connected to various grid protocols that compromise the grid functions. Specific hands-on experience in the classroom provided student teams from across a variety of

disciplines with a tangible platform to perform their experiments and develop their senior design projects on grid security. This ultimately allowed students to improve their knowledge base on cybersecurity concerns and recognize the effects of adverse events on critical infrastructure. We believe our efforts will eventually help the new generation towards becoming cybersecurity professionals, fulfilling the massive job vacancies in this critical area.

# 8 Acknowledgements

This work was supported in part by the U.S. National Science Foundation FW-HTF award 1840192 and multiple grants from the US Department of Energy. We acknowledge financial support from West Virginia University, which helped to establish this cyber-power lab. We also acknowledge the support from Schweitzer Engineering Laboratories.

# References

[1] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.

[2] N. M. Flores, H. McBrien, V. Do, M. V. Kiang, J. Schlegelmilch, and J. A. Casey, "The 2021 texas power crisis: distribution, duration, and disparities," *Journal of Exposure Science & Environmental Epidemiology*, pp. 1–11, 2022.

[3] A. M. Miller, "NC power station shootings show major vulnerability of u.s. power grid that requires action: Experts," Dec 2022. [Online]. Available: https://www.foxnews.com/us/nc-power-station-shootings-show-major-vulnerability-u-s-power-grid-that-requires-action-experts

[4] "Announcement of white house national cyber workforce and education summit," Jul 2022. [Online]. Available: https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/18/announcement-of-white-house-national-cyber-workforce-and-education-summit/

[5] A. K. Srivastava, C. H. Hauser, and D. E. Bakken, "Study buddies: Computer geeks and power freaks are learning smart systems together at washington state," pp. 39–43, 2013.

[6] A. K. Srivastava, A. L. Hahn, O. O. Adesope, C. H. Hauser, and D. E. Bakken, "Experience with a multidisciplinary, team-taught smart grid cyber infrastructure course," *IEEE transactions on power systems*, vol. 32, no. 3, pp. 2267–2275, 2016.

[7] J. Xie, J. C. Bedoya, C.-C. Liu, A. Hahn, K. J. Kaur, and R. Singh, "New educational modules using a cyber-distribution system testbed," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 5759–5769, 2018.

[8] T.-S. Chou, "An interactive learning system for cyber security education," in *2019 CIEC*, 2019.

[9] C. Foreman, M. Turner, and K. Perusich, "Educational modules in industrial control systems for critical infrastructure cyber security," in *2015 ASEE Annual Conference & Exposition*, 2015, pp. 26–573.

[10] S. M. Loo and L. Babinkostova, "Cyber-physical systems security introductory course for STEM students," 2020.

[11] P. Li, "Redesigning cyber security labs with immediate feedback," in *2022 ASEE Annual Conference & Exposition*, 2022.

[12] Y. Zhang and L. Li, "Integrating cyber infrastructure with physical laboratories," in *2013 ASEE Annual Conference & Exposition*, 2013, pp. 23–769.

[13] "CRITICAL INFRASTRUCTURE SECTORS," https://www.cisa.gov/critical-infrastructure-sectors, accessed: 2023-01-31.

[14] "Presidential policy directive – critical infrastructure security and resilience." [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[15] C. Zanocco, J. Flora, R. Rajagopal, and H. Boudet, "When the lights go out: Californians' experience with wildfire-related public safety power shutoffs increases intention to adopt solar and storage," *Energy Research & Social Science*, vol. 79, p. 102183, 2021.

[16] K. Chatterjee, V. Padmini, and S. Khaparde, "Review of cyber attacks on power system operations," in *2017 IEEE Region 10 Symposium (TENSYMP)*. IEEE, 2017, pp. 1–6.

[17] V. S. Rajkumar, M. Tealane, A. Ştefanov, A. Presekal, and P. Palensky, "Cyber attacks on power system automation and protection and impact analysis," in *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*. IEEE, 2020, pp. 247–254.

[18] "RTDS simulator," https://knowledge.rtds.com/hc/en-us/articles/8501418280855-RTDS-Simulator-Overview, accessed: 2023-01-31.

[19] H. M. Mustafa, M. Bariya, K. Sajan, A. Chhokra, A. Srivastava, A. Dubey, A. von Meier, and G. Biswas, "Rt-meter: A real-time, multi-layer cyber-power testbed for resiliency analysis," in *Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2021, pp. 1–7.

[20] S. H. Haji, S. Zeebaree, R. H. Saeed, S. Y. Ameen, H. M. Shukur, N. Omar, M. A. Sadeeq, Z. S. Ageed, I. M. Ibrahim, and H. M. Yasin, "Comparison of software defined networking with traditional networking," *Asian Journal of Research in Computer Science*, vol. 9, no. 2, pp. 1–18, 2021.

[21] J. Dearien and T. Watkins, "Migrating an Existing Network to OT SDN."

[22] A. Kalra, D. Dolezilek, J. M. Mathew, R. Raju, R. Meine, and D. Pawar, "Using software-defined networking to build modern, secure IEC 61850-based substation automation systems," *IET Conference Publications*, vol. 2020, no. CP771, 2020.

[23] "The PredictiveGrid Platform," https://www.pingthings.io/, accessed: 2023-01-31.

[24] V. Venkataramanan, A. Srivastava, A. Hahn *et al.*, "CP-TRAM: Cyber-physical transmission resiliency assessment metric," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5114–5123, 2020.

[25] S. Pandey, A. K. Srivastava, and B. G. Amidan, "A real time event detection, classification and localization using synchrophasor data," *IEEE Transactions on Power Systems*, vol. 35, no. 6, pp. 4421–4431, 2020.

[26] T. Crick, J. H. Davenport, P. Hanna, A. Irons, and T. Prickett, "Overcoming the challenges of teaching cybersecurity in uk computer science degree programmes," in *2020 IEEE Frontiers in Education Conference (FIE)*, 2020, pp. 1–9.

[27] T. Crick and J. H. Davenport, "Computer science degree accreditation in the uk: A post-shadbolt review update," in *Proceedings of the 4th Conference on Computing Education Practice*, 2020, pp. 1–4.

[28] P. G. Inglesant and M. A. Sasse, "The true cost of unusable password policies: password use in the wild," in *Proceedings of the sigchi conference on human factors in computing systems*, 2010, pp. 383–392.

[29] S. Palkar, "Industry-academia collaboration, expectations, and experiences," *ACM Inroads*, vol. 4, no. 4, pp. 56–58, 2013.

[30] J. L. Huff, J. Lönngren, T. Adawi, N. N. Kellam, and I. Villanueva, "Special session: Emotions in engineering education – a roadmap to possibilities in research and practice," in *2020 IEEE Frontiers in Education Conference (FIE)*, 2020, pp. 1–3.