This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2022-0609C

Towards Cyber-Physical Special Protection Schemes: Design and Development of a Co-Simulation Testbed Leveraging SCEPTRE™

Adam Summers*, Christopher Goes, Daniel Calzada,
Nicholas Jacobs, Shamina Hossain-McKenzie
Sandia National Laboratories
*asummer@sandia.gov

Zeyu Mao
Texas A&M University

***Abstract*—Unpredictable disturbances with dynamic trajectories such as extreme weather events and cyber attacks require adaptive, cyber-physical special protection schemes to mitigate cascading impact in the electric grid. A harmonized automatic relay mitigation of nefarious intentional events (HARMONIE) special protection scheme (SPS) is being developed to address that need. However, for evaluating the HARMONIE-SPS performance in classifying system disturbances and mitigating consequences, a cyber-physical testbed is required to further development and validate the methodology. In this paper, we present a design for a co-simulation testbed leveraging the SCEPTRE™ platform and the real-time digital simulator (RTDS). The integration of these two platforms is detailed, as well as the unique, specific needs for testing HARMONIE-SPS within the environment. Results are presented from tests involving a WSCC 9-bus system with different load shedding scenarios with varying cyber-physical impact.**

***Keywords*– real-time, cyber-physical system, cybersecurity, special protection schemes, machine learning, emulation, SCEPTRE**

I. Introduction

As the electric grid includes more and more smart grid (SG) technologies, traditional protection schemes and special protection schemes (SPS), also known as remedial action schemes (RAS), will not be enough to handle the unpredictable disturbances that will not be enough to handle the sort of unpredictable disturbances that, despite their growing numbers, are still referred to as high-impact low-frequency (HILF) events. Such unpredictable disturbances could either be man-made such as the Ukrainian cyber attacks [1] or weather related such as the Texas Winter Storm of 2021 [2]. SPS and other protection schemes that handle the isolation of faults to efficiently eliminate the cascading impacts and damage to equipment are essential to our grid but are not designed to handle these HILF events.

SPSs are typically deployed at the transmission level of the system due to the cost and are designed to operate at predefined system conditions. They have also been used at the distribution level more recently [3]. The predefined systems conditions could be better understood, but take significant of time to design and deploy; the triggering conditions and corrective action pair assignment requires extensive offline simulation studies in the planning stage [4], [5].

As the SG moves to incorporate the ever-increasing penetration of inverter-based resources (IBR), such as energy storage, photovoltaic (PV), and wind to the bulk electric system (BES), the need for adaptive SPSs grows. These distributed resources with communication-enabled features that can be controlled with SPSs are becoming more complex and time-consuming to engineer. The communication features of these devices present high-value, low-effort targets for cyber attacks that can quickly destabilize the grid [6]. This further increases the strain on SPSs to support the stability and reliability of our grid [7].

To develop the capabilities needed by future SPSs, our project team is developing a defensive, wide-area SPS that learns system conditions, mitigates cyber-physical consequences, and preserves grid operation under diverse predictable and unpredictable disturbances. This harmonized automatic relay mitigation of nefarious intentional events (HARMONIE)-SPS processes both cyber and physical data from both relays and out-of-band (OOB) measurements, learns actual system conditions to adapt

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government. This material is based upon work supported by the Sandia Laboratory Directed Research and Development Project # 222444; SAND NUMBER.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

to both predictable and unpredictable disturbances, and takes pre-emptive steps to prevent further cascading impact [8], [9].

SPSs can no longer solely be designed and tested in offline simulations. The work in [10]–[14] presents several cyber-physical system (CPS) testbeds that have been proposed. A PowerWorld simulation in [10] was used to analyze SCADA cybersecurity. The authors in [11] used a denial of service (DoS) attack with an RTDS for their testbed. In [12], the researchers performed several different cyber attacks in their testbed and evaluated impacts. In [13], a cyber-physical simulation environment is proposed to test SPS, however the details of the cyber emulation details are lacking. Authors in [14], developed a cyber-physical testbed using RTDS and OPNET and a Man-In-The-Middle attack (MITM) was used.

As the SG continues to incorporate IBRs and new communication features, the need for a flexible real-time cyber-physical (RTCP) emulation environment is needed. Many of the existing efforts focused on specific kinds of disturbances for their applications and high-level communication network modeling.For evaluating HARMONIE-SPS, we require a flexible cyber-physical environment in which a wide array of disturbances (e.g., cyber attack, extreme weather, EMPs) can be modeled and deep packet analysis of communication traffic can be performed.

Therefore, in this paper we detail the design and development of a real-time cyber-physical testbed that uses the RTDS simulator and a co-simulation environment with SCEPTRE™ [15] to enable modeling of a wide array of disturbances, high-fidelity modeling of both the cyber and physical systems, and real-time data sampling enabling HARMONIE-SPS machine learning as well as evaluation. Results are presented with disturbance data of varying cyber-physical cases using the WSCC 9-bus system.

Furthermore, this high-fidelity environment will enable the resilient development of additional grid cybersecurity and response tools, beyond HARMONIE-SPS. Both cyber and physical data streams can be monitored to understand response effectiveness and any additional burden, providing the necessary situational awareness for ensuring grid resilience with novel response measures.

This article is organized as follows. Section II focuses on the needs of a cyber-physical testbed for grid applications. Section III focuses on the design of the proposed experimental setup and the SCEPTRE™ environment. Section IV provides experimental results. Finally, Section V provides conclusions and plans for future work.

II. The Need for a Cyber-Physical Testbed

As SPSs are developed that depend on communications, testbeds that only enable physical (power system) data simulation do not suffice; there is a crucial need to incorporate the cyber (communication) data to understand the effects that predefined and unpredictable disturbances can have on a grid cyber system. Furthermore, performance of adaptive schemes such as the HARMONIE-SPS must be evaluated comprehensively with a wide array of disturbances and assessed with metrics from both the cyber and physical systems. For example, mitigations deployed by the HARMONIE-SPS must be evaluated to ensure communication latency is not increased significantly and/or power system operation is not interrupted.

A. Physical SPS

To date, SPSs have typically been designed to operate under physical system conditions; triggering conditions are identified and assigned to specific corrective actions during the planning stage using extensive simulation studies [7]. They generally take corrective action in three categories (typical triggering conditions listed):

1) Load Shedding
    a) The load is greater than generation
    b) Peak in demand due to weather
    c) Reduced production of renewable energy due to weather conditions
2) Generation Tripping
    a) Adjusting MW and Mvar output
3) Line Tripping
    a) Excessive line loading
    b) Topology changes

Each of these physical SPS corrective actions is designed for a predefined system triggering condition that if corrective action is not taken would result in the system becoming unstable.

B. Cyber SPS

At present, cyber SPSs do not exist; instead, intrusion detection and/or prevention systems may be installed in a utility's enterprise network to act on detected events [16]. Encryption and other defense tools can also be installed to motivate a defense-in-depth approach. Usually, cyber-side mitigations operate in a predefined, signature-based playbook manner in the IT network and do not consider physical system impact.

Thus, for cyber events in the electric grid, whether malicious or inadvertent, we must consider cyber-physical data to ensure impact to either domain is not sustained. Furthermore, there is a need for adaptive cyber-physical corrective actions to address unpredictable disturbances.

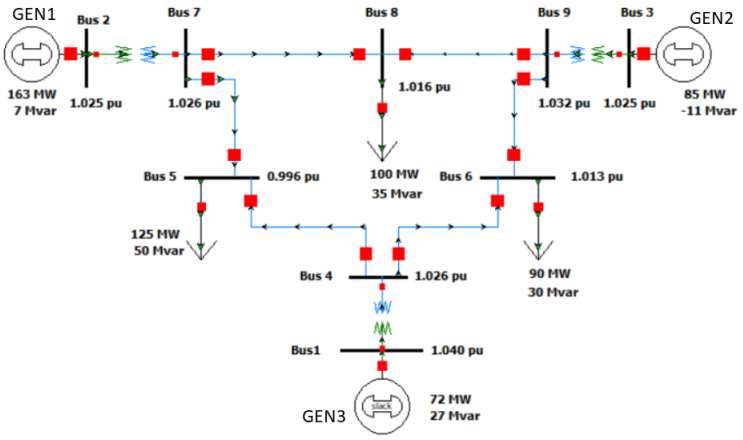

Fig. 1: WSCC 9-bus system oneline diagram.

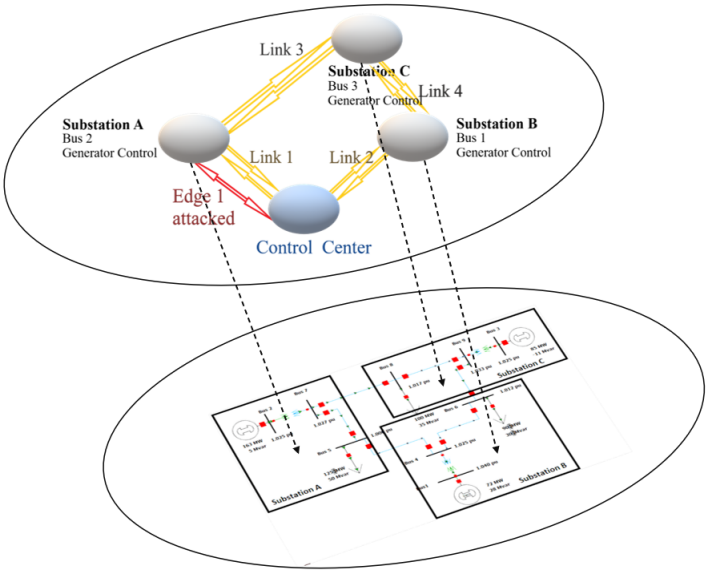

Fig. 2: WSCC 9-bus system oneline diagram and representative communication network.

C. Cyber-Physical SPS

With the advent and integration of novel smart-grid technologies that broaden the cyber attack surface, the rise of unpredictable disturbances such as EMPs, and the looming presence of extreme weather events, a next-generation SPS with the following attributes is needed:

1) A SPS that can adapt to unpredictable events (without predefined conditions) and effectively respond to limit/eliminate the disruption quickly
2) A SPS that is cyber-physical in analyzing collected data and taking response actions; it is no longer sufficient for a SPS to process only physical power system data and solely take physical-side actions; cyber-side actions are necessary to eliminate malicious compromise
3) A SPS that extends the use of protective relays from fault isolation to also adaptively learning system conditions, preventing cyber attack propagation, and taking proactive actions to prevent compromise within the relay set itself

To meet the needs of future SPSs, the project team proposed the HARMONIE-SPS that learns system con-

ditions, mitigates cyber-physical consequences, and preserves grid operation under diverse predictable and unpredictable disturbances [9]. With this increased situational awareness and proactive control response approach, the HARMONIE-SPS can greatly improve the resilience of the electric grid against cyber-physical disturbances, whether they are malicious or inadvertent. The remainder of the paper will detail the design and development of a cyber-physical emulation environment to test the HARMONIE-SPS approach.

III. The HARMONIE-SPS Cyber-Physical Testbed Design and Development

A. System of Study

As SPSs are used at the transmission level of the grid, a simplified model of a portion of the US electric grid was selected to build the initial HARMONIE-SPS testbed. This does not limit the HARMONIE-SPS testing to this use case, but is used for simplified demonstration purposes. The Western System Coordinating Council (WSCC) 9-bus system shown in Fig. 1 was modeled in the RTDS. The RTDS is a real-time digital simulator that enables dynamic power system modeling and hardware-in-the-loop (HIL) testing capabilities [17]. The model has several different voltages levels, generation sources, and controllable loads; making it an ideal test case to implement a cyber-physical system. The model is broken into three different zones, as indicated in Fig. 2, and 9 phasor-measurement units (PMUs) placed at each of the 230 kV buses.

A representative communication network was developed using an automated approach [18]; the communication network developed for the WSCC 9-bus system is shown in Fig. 2. The system is separated into three different substations. Substation A includes generator 1, Bus 2, Bus 7, and Bus 5. Substation B includes generator 3, Bus 4, Bus 6, and Bus 1. Substation C includes generator 2, Bus 8, Bus 9, and Bus 3.

B. RTDS and SCEPTRE™ Communications and I/O

The RTDS is able to support several different communication protocols such as C37.118, Sampled Values, Sockets, DNP3, and Modbus. For this use case, the C37.118 and Sockets protocols are used to send and receive data. This data is communicated to the SCEPTRE™ co-simulation environment. How this data is ingested within SCEPTRE™ will be explained in the next section. The RTDS is capable of supporting analog inputs and outputs, as shown in Fig. 3. In our use case, an SEL 451 protective relay is connected via these analog inputs to form an HIL simulation.

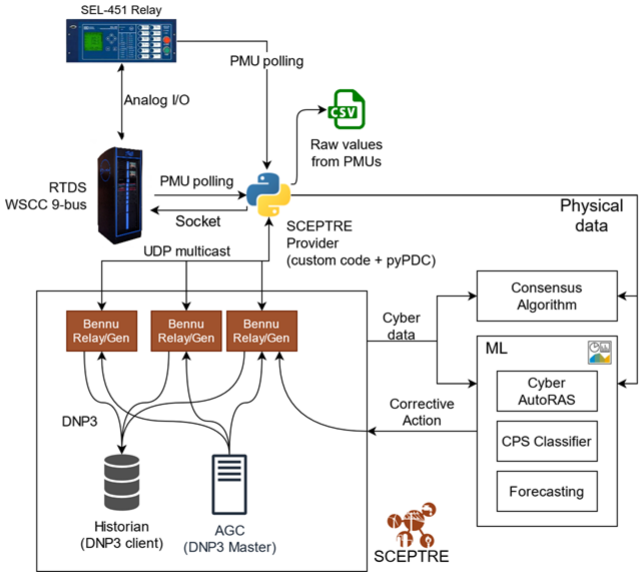

Fig. 3: SCEPTRE and RTDS integration design.

C. SCEPTRE™ Implementation

SCEPTRE™ is an application that uses an underlying network emulation and analytic platform (Emulytics™) to model, simulate, emulate, test, and validate control system security and process simulations. Traditionally, tools and techniques for simulating and emulating control system field devices have been limited because the physical processes such as power system operation are omitted. SCEPTRE™ integrates the device and process simulations and enables a system capable of representing realistic responses in a physical process as events occur in the control system and vice versa. HIL device experiments are also enabled [19].

D. Integration Approach for RTDS and SCEPTRE

For integrating the RTDS and SCEPTRE™ platforms to enable cyber-physical emulation and enable real-time cyber-physical data extraction for HARMONIE-SPS training and testing, protocol communications are being leveraged to link the two platforms. As shown in Fig. 3, the SCEPTRE™ provider running in the SCEPTRE™ will poll the RTDS for data via the C37.118 protocol, implemented using pyPMU [20]. The provider then converts this data into a protocol-agnostic format and sends it to the virtual SCEPTRE™ relays via UDP multi-cast. Depending on their configuration, the virtual relays will translate it to a communication protocol. To write back into the RTDS, the RTDS-proprietary socket communication protocol [21] will be utilized. The system is deployed on a server running SCEPTRE™ networked to the RTDS and with the HARMONIE-SPS SCEPTRE™ topology deployed.

E. HARMONIE-SPS Machine Learning Training and Testing Needs

To handle the unpredictable HILF disturbances, the HARMONIE-SPS testbed includes several different types of algorithms for real-time analysis. The consensus algorithm relay voting scheme approach [8] will ingest both the cyber and physical data to arrive on a distributed relay voting response to different disturbances. Additionally, different machine learning (ML) algorithms are being developed and tested, such as graph neural networks and transformer models, with the cyber and physical data for the classify system conditions to inform response to these predictable and unpredictable disturbances; more details on the HARMONIE-SPS ML framework can be found on [9] that can classify the system into four different classes: normal operations, cyber disturbances, physical disturbances, and cyber-physical disturbances.

The next section documents our use of the cyber-physical testbed to explore several case studies with varying impact to cyber-physical data. The results demonstrate the collection of streaming cyber-physical data and its successful collection in the environment's historian. This data can then be used for training the ML algorithms as well as testing the real-time analysis capabilities.

IV. Case Studies

For these use cases, we focused on Bus 8 in Fig. 1 that is connected between two transmission lines and has a 100 MW and 35 Mvar load connected. The load could be remotely controlled as a corrective action deployed from the HARMONIE-SPS.

A. Physical Event: Load Drop

To test that the closed loop connection between the RTDS and SCEPTRE™ was configured correctly, a breaker trip command was sent from one of the Bennu VMs (Substation C RTU) using a SCEPTRE™ command (pybennu-probe) to open the breaker at Bus 8 simulating a load drop.

B. Results

The results of the HARMONIE-SPS cyber-physical testbed for this load drop scenario show that the WSCC 9-bus system has been successfully deployed in the RTDS with the C37.118 protocol connections to SCEPTRE™ completed. Fig. 4, shows the RMS per unit Bus 6 voltages of the use case when the load at Bus 8 is disconnected by a corrective response such as a load tripping scheme.

Thus, the integration of RTDS and SCEPTRE™ is successful as this load shedding impact to the WSSC 9-bus system can be observed from either the RTDS or SCEPTRE™ system due to the emulation environment design described in Fig. 3.

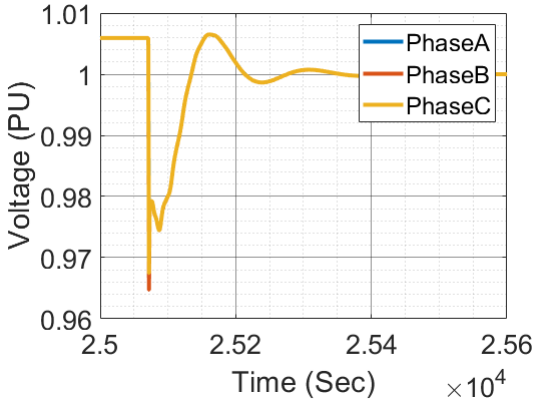

Fig. 4: Bus 6 RMS Voltages

C. Cyber Event: Loss of C37.118 At Substation C

For this use case, all of the PMU connections have been dropped at Substation C. This could represent an equipment failure or a malicious event (e.g., denial of service attack). This loss of system visibility could prevent an SPS from operating correctly. However, the use of ML algorithms to help classify the system into four different categories: normal operations, cyber disturbances, physical disturbances, and cyber-physical disturbances using the cyber data and the framework in [9] and subsequent adaptive response, increases the system resilience.

D. Results

Using the SCEPTRE™ platform to drop several of the PMU connections at a virtual router allows us to analyze different system SPS that could be configured. The results of this use case are shown in Fig. 5. The vertical red line in Fig. 5 indicates when the router went offline. The cyber data can be collected in real-time allowing for a deep packet analysis capability of grid cyber data. This deep packet analysis can be performed by the ML algorithms deployed in HARMONIE-SPS and/or IDS tools such as Zeek or Snort for other applications.

E. Cyber-Physical Event: Loss of Critical Cyber Equipment At Substation C and with Load Drop

This use case joins the previous two cases together, however the load drop command is sent from an unknown location as shown in Fig. 2 as the Edge 1.

F. Results

The results shown in Fig. 6 and Fig. 7 depict the deep packet inspection of the cyber data and physical data as viewed from the control center. The vertical red line in Fig. 6 indicates when the router went offline. A cyber-physical scenario has been successfully deployed and the

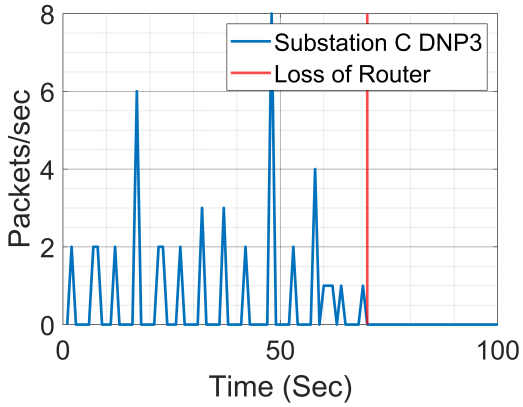

Fig. 5: DNP3 Packet Capture From The Control Center of Substation C

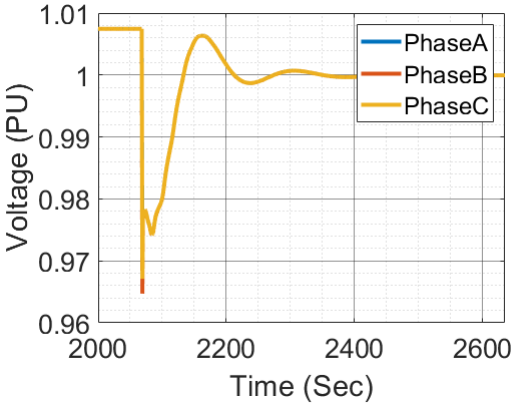

Fig. 7: Bus 6 RMS Voltages

resulting data can be used to train ML algorithms to mitigate such a scenario.

Furthermore, with insight into both the real-time cyber and physical data streams, we can assess the performance of mitigations deployed by HARMONIE-SPS for any type of disturbance (cyber-only, physical-only, cyber-physical). For response mechanisms such as SPSs, it is important to consider the impact of the response to both the grid operation (e.g., limit violations, stability) and communication network (e.g., latency, bandwidth).

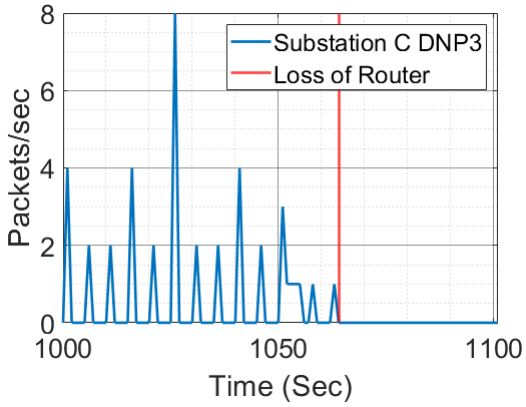

Fig. 6: DNP3 Packet Capture From The Control Center of Substation C

V. Conclusions

In this paper, the HARMONIE-SPS cyber-physical emulation testbed approach for testing an adaptive, cyber-physical SPS has completed the process of connecting the RTDS and SCEPTRE™ co-simulation environments. Results for three different use cases are presented demonstrating a successful connection and data transfer between the RTDS and SCEPTRE™ platforms.

The cyber-physical scenarios explored in the testbed demonstrated the high-fidelity impact and extraction of cyber-physical data; specifically, this testbed provides deep packet analysis capability of grid cyber data as well as analysis of power system dynamics. Therefore, the developed testbed enables more effective and resilient development of grid cybersecurity tools such as HARMONIE-SPS. Additionally, the ability to extract cyber-physical time-series data streams for continuous operation, with and without disturbances, is a significant advantage for training machine learning algorithms, as used in HARMONIE-SPS.

Future work for this testbed will continue implementing different disturbances for training and testing HARMONIE-SPS as well as incorporating additional hardware-in-the-loop.

References

[1] "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, 2016.

[2] "Ercot winter storm generator outages by cause," Nov 2021. [Online]. Available: http://www.ercot.com/content/wcm/lists/226521/ERCOT_Winter_Storm_Generator_Outages_By_Cause_Updated_Report_4.27.21.pdf

[3] M. R. Duff, P. Gupta, D. Prajapati, and A. Langseth, "Utility implements communications-assisted special protection and control schemes for distribution substations," in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, 2017, pp. 1–11.

[4] P. Anderson and B. LeReverend, "Industry experience with special protection schemes," *IEEE Transactions on Power Systems*, vol. 11, no. 3, pp. 1166–1179, 1996.

[5] H. Li, K. Shetye, T. Overbye, K. Davis, S. Hossain-McKenzie, "Towards the automation of remedial action schemes design," in *Proceedings of the 54th Hawaii International Conference on System Sciences*, 2021.

[6] P. Mazzei, I. Penn, F. Robles, "With earthquakes and storms, puerto rico's power grid can't catch a break," *The New York Times*, 2020.

[7] H. Li, K. Shetye, S. Hossain-McKenzie, K. Davis, and T. Overbye, "Investigation of Automated Corrective Actions for Special Protection Schemes," SAND2020-9602, Sandia National Laboratories, Tech. Rep., 2020.

[8] N. Jacobs, A. Summers, S. Hossain-McKenzie, D. Calzada, H. Li, Z. Mao, C. Goes, K. Davis, and K. Shetye, "Next-generation relay voting scheme design leveraging consensus algorithms," in *2021 IEEE Power and Energy Conference at Illinois (PECI)*, 2021, pp. 1–6.

[9] S. Hossain-McKenzie, D. Calzada, N. Jacobs, C. Goes, A. Summers, K. Davis, H. Li, Z. Mao, T. Overbye, and K. Shetye, "Adaptive, cyber-physical special protection schemes to defend the electric grid against predictable and unpredictable disturbances," in *2021 Resilience Week (RWS)*, 2021, pp. 1–9.

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

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

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

[13] A. Mallikeswaran, T. Ashwarya, S. Niddodi, A. Srivastava, D. E. Bakken, and P. Panciatici, "Cyber physical simulation and remote testing of remedial action schemes," in *2016 IEEE/PES Transmission and Distribution Conference and Exposition (T D)*, 2016, pp. 1–5.

[14] B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, "Implementing a real-time cyber-physical system test bed in rtds and opnet," in *2014 North American Power Symposium (NAPS)*, 2014, pp. 1–6.

[15] "Sceptre." Aug 2016. [Online]. Available: https://www.osti.gov/servlets/purl/1376989

[16] C. Lai, A. R. Chavez, C. B. Jones, N. Jacobs, S. Hossain-McKenzie, J. B. Johnson, and A. Summers, "Review of intrusion detection methods and tools for distributed energy resources." Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2021.

[17] R. Kuffel, J. Giesbrecht, T. Maguire, R. Wierckx, and P. McLaren, "Rtds-a fully digital power system simulator operating in real time," in *Proceedings 1995 International Conference on Energy Management and Power Delivery EMPD '95*, vol. 2, 1995, pp. 498–503 vol.2.

[18] M. Soetan, Z. Mao, and K. Davis, "Statistics for building synthetic power system cyber models," in *2021 IEEE Power and Energy Conference at Illinois (PECI)*, 2021, pp. 1–5.

[19] T. R. Camacho-Lopez, "Sceptre." 8 2016. [Online]. Available: https://www.osti.gov/biblio/1376989

[20] S. Šandi, T. Popovic, and B. Krstajic, "Python implementation of ieee c37.118 communication protocol," *ETF Journal of Electrical Engineering*, vol. 21, pp. 108–117, 12 2015.

[21] "Gtnetx2: The rtds simulator's network interface card ..." [Online]. Available: https://knowledge.rtds.com/hc/en-us/articles/360034788593-GTNETx2-The-RTDS-Simulator-s-Network-Interface-Card