Adaptive, Cyber-Physical Special Protection Schemes to Defend the Electric Grid Against Predictable and Unpredictable Disturbances

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

Katherine Davis, Hanyue Li, Zeyu Mao,
Thomas Overbye, Komal Shetye
Texas A&M University

***Abstract*—Special protection schemes (SPSs) safeguard the grid by detecting predefined abnormal conditions and deploying predefined corrective actions. Utilities leverage SPSs to maintain stability, acceptable voltages, and loading limits during disturbances. However, traditional SPSs cannot defend against unpredictable disturbances. Events such as cyber attacks, extreme weather, and electromagnetic pulses have unpredictable trajectories and require adaptive response. Therefore, we propose a harmonized automatic relay mitigation of nefarious intentional events (HARMONIE)-SPS that learns system conditions, mitigates cyber-physical consequences, and preserves grid operation during both predictable and unpredictable disturbances. In this paper, we define the HARMONIE-SPS approach, detail progress on its development, and provide initial results using a WSCC 9-bus system.**

***Keywords*–cyber-physical system, cybersecurity, special protection schemes, relay voting schemes, consensus algorithms, machine learning, emulation**

I. Introduction

Protection schemes are vital to the continuous, reliable operation of the electric grid. There exist a variety of protection schemes that coordinate protective relays during power system faults and seek to isolate and clear the faults quickly and efficiently to prevent any sustained damage and cascading impact. Extending the focus from isolating and clearing faults, SPSs protect the grid by detecting predefined abnormal conditions and deploying predefined corrective actions in a playbook manner. It is important to note that SPSs and remedial action schemes (RASs) terminology is often used interchangeably [1].

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; SAND2021-12162 C.

SPSs prioritize reliability and seek to maintain stability, acceptable voltages, and loading limits during disturbances, essentially operating within the respond and recover functions of National Institute of Standards and Technology's Cybersecurity Framework [2]. Unlike typical protection schemes, SPSs can take actions beyond the isolation of a fault and include changes to demand, generation, and system configuration.

However, it no longer suffices for SPSs to focus solely on predefined disturbances and reliability. Resilience and unpredictable disturbances such as electromagnetic pulses (EMPs), extreme weather, and malicious events threatening national security must be considered. Hurricane Maria in Puerto Rico revealed the fragility of grid physical infrastructure, which suffered severe damage and continues to require significant restoration effort. It showed how quickly cascading failures can destabilize even undamaged equipment and the dependency and interconnectedness of critical infrastructure [3].

Cyber attacks targeting grid operations are increasing in frequency and intensity, as exemplified by the calamitous 2015 and 2016 cyber attacks to the Ukrainian grid [4]. Furthermore, with the increasing penetration of distributed energy resources (DER) such as solar photovoltaic (PV) systems and wind farms, new technologies are being integrated and connected to the bulk power system. These grid-edge devices, with novel communication and automation functionalities, are also becoming targets to cyber attacks and can cause detrimental impact propagation as DER penetration increases [5].

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

2021 Resilience Week (RWS) | 978-1-6654-2905-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/RWS52686.2021.9611801

IEEE 978-1-6654-2905-4/21/$31.00 ©2021 IEEE
Authorized licensed use limited to: Texas A&M University. Downloaded on April 05,2024 at 20:15:36 UTC from IEEE Xplore. Restrictions apply.

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, we propose 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 will meet the needs stated above by processing both cyber and physical data from both relays and out-of-band (OOB) measurements, learning actual system conditions to adapt to both predictable and unpredictable disturbances, and performing proactive response actions to prevent further cascading impact.

Furthermore, the HARMONIE-SPS will leverage the distributed sets of protective relays, within different zones, to derive classification of the system conditions and respond to disturbances. 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 it is intentionally malicious or inadvertent.

In this paper, we detail our initial HARMONIE-SPS approach, including the machine learning framework, cyber-physical testbed development, and consensus algorithm-based relay voting scheme. Preliminary results are presented with disturbance data (both cyber and physical) using a WSCC 9-bus system.

II. SPS Background

According to the Western Electricity Coordination Council (WECC), there are four common elements for the design of SPS/RAS: arming criteria, initiating conditions, actions taken, and time requirements [6]. The arming criteria are critical system conditions for which a step-wise SPS should be ready to take action when required. The initial conditions are the contingencies that have been known to cause violations of reliability and stability standards, which will initiate the SPS corrective action if the scheme is armed. The initial conditions can be event-based, parameter-based, response-based, or the combination of the above.

Event-based schemes directly detect outages and/or fault events and initiate actions to fully or partially mitigate the event consequence. Parameter-based schemes measure variables for which a significant change confirms the occurrence of a critical event. Response-based schemes monitor system response during events and disturbances and incorporate a closed-loop process to react to actual system conditions [7]. The work of [8] finds that most SPS in the WECC system initiate upon changes to system topology, with very few being triggered by system condition changes.

A. Existing Online SPS Efforts

Many research efforts, from both industry and academia, have gone into improving the flexibility and dynamics of SPS implementation. In [9], an event-based method was proposed to enhance SPS that are created to address specific frequency and voltage instability issues. Using transient energy analysis, the conventional SPS implementation can be adjusted with flexible triggering thresholds [10], and also adaptive corrective actions [11]. To mitigate the risk of voltage instability and voltage collapse, BC Hydro developed a methodology to determine the magnitude of load shedding based on real-time measurement data [12].

Recent work [13] by the Pacific Northwest National Laboratory (PNNL) proposed an approach to adaptively set the arming parameters of existing SPS based on realistic and near real-time operation conditions. In collaboration with PacifiCorp and Idaho Power Company, a prototype named Transformative Remedial Action Scheme Tool (TRAST) was developed with advanced computing methods for adaptively setting SPS coefficients with the consideration of realistic and near real-time operation conditions. The Jim Bridger RAS, owned and operated by PacifiCorp, was used as the case study for testing and validating the methodology and prototype.

The TRAST tool performs statistical analysis for full-year supervisory control and data acquisition (SCADA) set provided by utilities that contain essential variables for the existing SPS model. Correlation analysis and regression is performed between these variables, as well as with temporal data such as season and month and power flow data from state estimator cases. A machine learning framework was developed to update the RAS coefficients; full details on the framework can be found in [13]. To summarize, this online SPS tool is automated in the sense that the parameters adapt to real-time conditions, however the design of the underlying SPS itself is manual. The other key factor is the vast amount of real system data (measurements and models) needed for the entire framework, spanning multiple entities and even years.

Overall, although the need for an adaptive SPS has been recognized, especially for the SPS development and triggering phases, adaptive and cyber-physical SPSs have not been proposed. The grid is increasingly cyber-

Authorized licensed use limited to: Texas A M University. Downloaded on April 05,2024 at 20:15:36 UTC from IEEE Xplore. Restrictions apply.

physical and impact from either domain can easily propagate to the other – cyber-physical disturbances must be protected against for improved grid resilience.

III. HARMONIE-SPS Approach

For increased grid resilience, we hypothesize that an adaptive and reactive cyber-physical SPS is necessary for defending against diverse predictable and unpredictable disturbances, inadvertent or malicious. Therefore, we propose a defensive, wide-area SPS that learns system conditions, mitigates cyber-physical consequences, and preserves grid operation during both predictable and unpredictable disturbances.

HARMONIE-SPS will:

- Detect and defend against cyber attacks that do not fit predefined abnormal conditions by using machine learning (ML) classification and anomaly detection algorithms,
- incorporate intrusion detection system (IDS) and out-of-band (OOB) data for increased situational awareness, and
- proactively respond to cyber-physical compromises by deploying distributed control algorithms and taking cyber-side actions (e.g., rejecting setting/firmware changes) to reduce and/or eliminate system impact.

An overview of the approach is shown in Fig. 1. HARMONIE-SPS will prioritize selectivity, speed, and security using ML algorithms to classify system conditions, as detailed in the next section.

A. Prioritizing Speed, Security, and/or Selectivity

Utilizing the classification of system conditions, HARMONIE-SPS will decide to prioritize selectivity, speed, or security; additionally, a combination could be selected. If a relay within a zone is compromised, selectivity will be enabled by deploying the CA-based voting scheme approach that considers diverse zone relays and OOB data, as detailed in Section VI.

Unlike traditional relay voting schemes that simply compare tripping decisions, the proposed CA-based voting scheme would account for inter-relay relationships in different zones and provide the ability to assign weights depending on the disturbance location and indication of specific relay compromise or failure (e.g., assign zero weight to that relay's vote). Thus, selectivity can be achieved by ensuring relay status and relationships are incorporated into the voting for high confidence in relay actions for the most up-to-date system conditions.

If detrimental system conditions are observed, speed will be prioritized by taking proactive actions such as switching to backup protection schemes to reduce impact propagation and/or deploying reduced-order voting scheme to achieve both speed and selectivity. Backup protection schemes could compensate for compromised/failed relay zones and provide increased protection to critical grid components such as generators and transformers.

When HARMONIE-SPS prioritizes speed, methods to quickly reduce/eliminate system impact and provide the most protection possible are needed. For both selectivity and speed, physical mitigations could also be deployed to maintain system operation. This could include distributed control approaches that employ power system devices such as distributed flexible AC transmission system (D-FACTS) and design their response to limit disturbance impact [14], [15]. Distributed decision-making algorithms, such as alternating direction method of multipliers (ADMM), could be explored as a powerful distributed convex optimization approach for making control decisions between distributed devices in response to system disturbances [16].

Lastly, security is enhanced with HARMONIE-SPS by: 1) taking proactive actions to minimize impact propagation, 2) supplying relay data to augment analysis and aid IDSs in identifying the disturbance, and 3) providing confidence in tripping decisions with the novel CA-based voting scheme. The proactive actions taken by HARMONIE-SPS include both cyber-side and physical-side mitigations. The physical-side mitigations encompass the distributed control approaches and switching to backup protection schemes whereas the cyber-side actions could include rejecting further firmware/setting changes, communicating relay compromise/malfunction to other peer relays, and restoring backup device configuration files. Additionally, if an IDS exists in the system, HARMONIE-SPS's findings on abnormal relay behavior (e.g., co-located, different zone relay measurements do not match) and classification results can be used to supplement the IDS data collection and analysis.

B. Evaluating HARMONIE-SPS

The high-fidelity cyber-physical emulation environment will be constructed using SCEPTRE™ and a real-time digital simulator such as RTDS. SCEPTRE™ is Sandia's industrial control system (ICS) modeling platform that enables modeling of different ICS devices (virtual and hardware) such as protective relays and programmable logic controllers, network components (e.g., gateways, switches, servers), actual ICS communication protocols (e.g., Modbus, DNP3, IEC 61850), and physical end processes (e.g., power system simulations). The RTDS will be used to model the physical end process and enable connecting protective relays both virtually and as hardware-in-the-loop (HIL). This emulation environment is discussed in Section V.

In this manner, metrics can be collected to verify if HARMONIE-SPS reduced or eliminated system impact

Authorized licensed use limited to: Texas A M University. Downloaded on April 05,2024 at 20:15:36 UTC from IEEE Xplore. Restrictions apply.

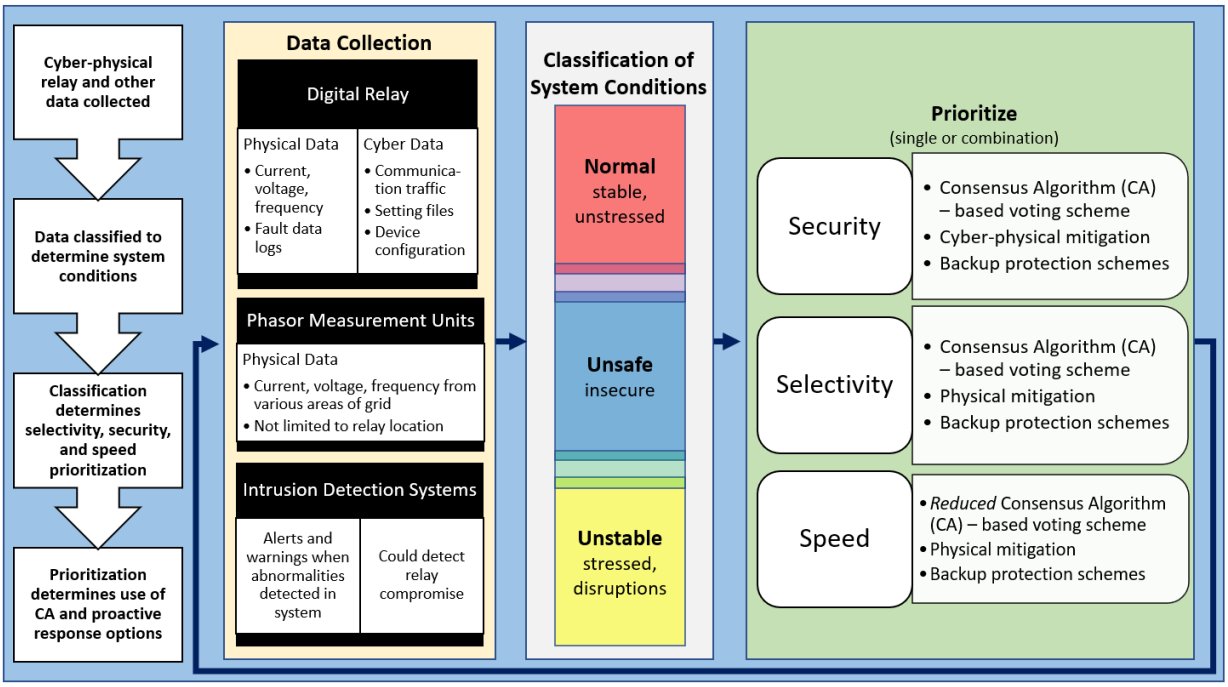

Fig. 1: Overview of HARMONIE-SPS Approach with cyber-physical data collection, classification of system conditions, and priority-informed response.

from a disturbance, malicious or inadvertent, and that network burden was not worsened with the application of HARMONIE-SPS (e.g., increased latency, dropped packets). Malicious cyber-physical disturbance scenarios are being developed to reflect a wide range of attacks and based on real-world events (e.g., using MITRE ATT&CK framework [17]).

IV. Machine Learning Framework

At a high level, the machine learning approach for HARMONIE-SPS converts incoming data (cyber data or physical data) into a graph of interconnected nodes, where each edge is a flow of information with an associated timestamp. After the whole capture is split into subgraphs using 24-second sliding windows[1], the algorithm relies upon two deep learning architectures to obtain an overall representation of the system state in each window:

- A Graph Convolutional Neural Network (GNN), which applies deep learning to the structure of interconnected nodes in the subgraph, and
- A Recurrent Neural Network (RNN), which applies deep learning to the temporal ordering of the edges in the subgraph.

[1]24 seconds was chosen somewhat arbitrarily. If the window is too small, we might miss relevant context to understand the system state, and if the window is too large, the network will run more slowly and we will have more trouble localizing the disturbance.

Using the GNN and RNN in tandem would theoretically allow for representing the changing system state over time with the RNN while understanding the connectivity of the cyber or physical network with the GNN, especially in complex networks. First, the GNN operates by passing four rounds of messages between edges, and the resulting edge vectors are passed to the RNN to encode temporal information.

To assess the classification of different system conditions within a cyber-physical grid system, we add a classification layer onto the network that predicts two binary labels: whether a cyber disturbance is occurring and whether a physical disturbance is occurring. This combination of two binary labels allows our model to categorize the system state into four categories:

1) Normal operations
2) Cyber-only disturbances
3) Physical-only disturbances
4) Cyber-physical disturbances

A. Initial Classification Results

To test our approach, we utilized the WSCC 9-bus system within Texas A&M University's co-simulation-based cyber-physical grid testbed, shown in Fig. 2, and modeled it under different disturbance scenarios [18]. The disturbances tested were:

1) Denial of service (cyber-only)
2) Single line-to-ground fault (physical-only)

Authorized licensed use limited to: Texas A M University. Downloaded on April 05,2024 at 20:15:36 UTC from IEEE Xplore. Restrictions apply.

TABLE I: Preliminary Results for HARMONIE-SPS ML Model (Cyber anomaly AUC / Physical anomaly AUC)

	With Pretraining	**No Pretraining**
900 windows	0.74 / 0.92	0.95 / 0.92
100 windows	0.49 / 0.64	0.52 / 0.60

3) Tripping command injection (cyber-physical)
4) Time-delay attack (cyber-physical)

A total of 50 network and physical data captures of various 2-minute scenarios of each of the listed disturbances were used to test the machine learning approach. For the experiments, we partitioned all scenarios into 30 for training, 10 for validation and model selection, and 10 for testing. These were then split into their respective sliding windows.

We ran experiments varying the size of the training data and comparing the results when using a model that has already been pretrained using some basic predefined perturbations versus a model that had not been pretrained. Table I contains the results of these experiments for training with 900 windows (30 scenarios) and with 100 windows ($\sim$3.3 scenarios). We used the area under the receiver operator curve (AUC) as our metric because it identifies how well a model's predictions split the two classes apart and does not require a predefined threshold to convert real-valued confidence scores into a discrete class prediction.

From these results, we can see that using the full training data, our model can differentiate between disturbances and normal behavior. We also hypothesize that the pretraining step either adds nothing to or even mildly hinders the performance of the model, especially when identifying cyber anomalies. We attribute this to a domain shift between the inputs during the pretraining step, where perturbed graphs are given to the model, and the training step, where unmodified graphs are given to the model. That is, our current approach is closer to transfer learning than pretraining. We also provide a confusion matrix for the best model (using all 900 training windows with no pretraining) in Fig. 3.

In Fig. 4, we use our best model (trained on all 30 scenarios with no pretraining) to plot the predicted anomaly scores for each scenario in the test set. Since our approach uses 24-second sliding windows, all windows ending between 00:00:59 and 00:01:23 will contain the disturbance which occurs at 00:00:59 (blue vertical line). Note that some scenarios have cyber disturbances only in the middle of the capture, which is why some cyber anomaly scores drop to nearly 0 after 00:01:24.

In these plots, we see that our deep learning approach can roughly identify when a disturbance occurs and whether the disturbance is in the cyber, physical, or a cyber-physical event.

B. Overall Machine Learning Framework Next Steps

There are several next steps for the machine learning component of the HARMONIE-SPS. First, we plan to incorporate our forecasting algorithm for imputing missing data and the support vector machine for identifying violations in the underlying physical system.

Second, we intend to improve our data by obtaining more scenarios to use for training, validation, and testing, obtaining more diverse scenario types. This will give us a better understanding of the strengths and shortcomings of our approach and help us identify solutions. We would also be able to use this as a metric for how well our network generalizes to previously unseen scenario types. Along the same vein, we would like to use cross-validation to obtain more predictions, thus reducing bias and variance in our metric values such as AUC or F1 score. We would also benefit from more rigorous labeling of our data: currently, we assume that all disturbances happen at exactly $t = 60s$. This was the target when generating our experimental data, but due to some synchronization issues during the capturing of the data, the disturbance may happen within a few seconds of that instead. By obtaining more precise timing in this dataset or future captures, we can increase our confidence in our training data and validation metrics.

Third, we would like to gain better insight into the model itself by inspecting and interpreting the GNN's output. Our data is complex and noisy, and understanding what our network is learning will be a critical step in refining it. We would also like to give more thought to why the pretraining approach has not yielded the results we were expecting and to either mitigate any issues or disregard the pretraining approach entirely.

In conclusion, our machine learning framework for identifying known disturbances in the cyber network or physical power system shows promise. By continuing to improve upon our existing approach, we believe this will be a viable solution to the problem of using machine learning to understand the holistic, cyber-physical state of a power system and recommend action through HARMONIE-SPS.

C. Automated Corrective Action Assignment

In Section II A., the manual process of assigning suitable corrective actions to SPS triggering conditions was discussed and how traditionally this requires many offline simulations and extensive planning studies. Thus, the research team is also developing a more flexible, computationally efficient approach for determining SPS corrective actions by automatically generating the triggering condition and correction action pairs based on the identified need for a new SPS creation. This procedure

Authorized licensed use limited to: Texas A M University. Downloaded on April 05,2024 at 20:15:36 UTC from IEEE Xplore. Restrictions apply.

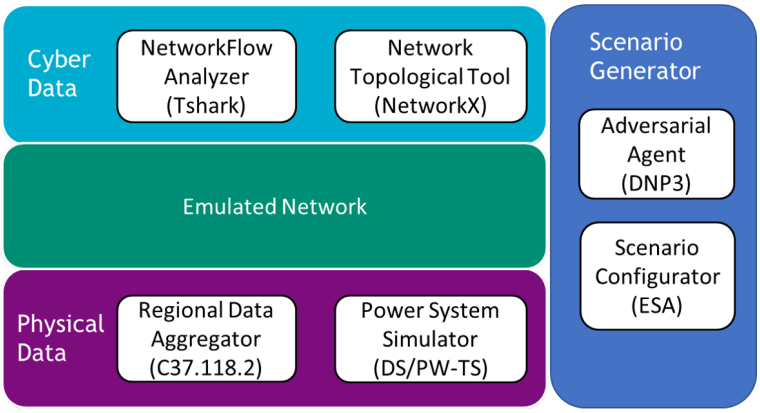

Fig. 2: Texas A&M University's cyber-physical grid testbed used to model different disturbance scenarios with the WSCC 9-bus system.

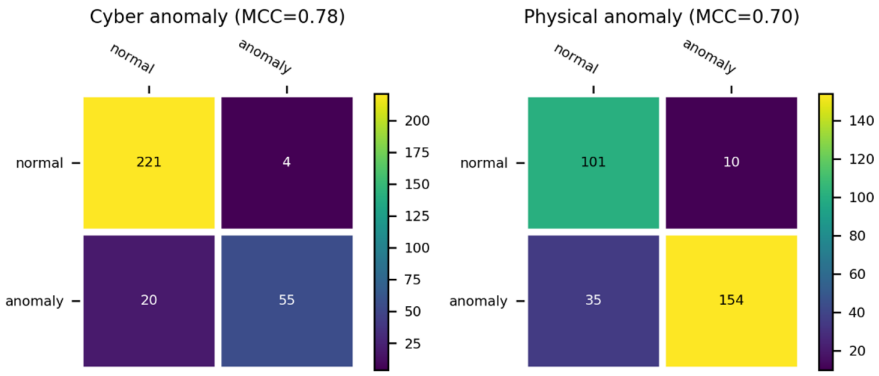

Fig. 3: Confusion matrices for identifying cyber and physical disturbances on the test data using a threshold of 0.5. Matthew's Correlation Coefficient (MCC) is used to assess the quality of the predictions. Rows correspond to actual classes and columns correspond to predicted classes.

and its results with a 2000-bus synthetic power system are detailed in [19], [20].

To extend the pairing of triggering conditions and corrective action pairs, we are working on using machine learning to identify when a triggering condition has been encountered. Presently, we are developing an approach to cluster (using hierarchical clustering algorithm) violation elements resulting from contingency analysis applied to the WSCC 9-bus system (22,000 scenarios were generated and a subset was sampled) [21]. The violations within the same cluster can then be addressed with one corrective action, as identified using a support vector machine (SVM) approach. Ultimately, the outputs of the SVM will be inputted into the GNN and RNN framework to confirm the corrective action.

This work is currently focusing on the physical power system but will be extended to the cyber domain as well in future work (e.g., network triggering conditions and corrective actions such as rerouting packets, restoring default device configuration).

V. Cyber-Physical Testbed Development

A high-fidelity cyber-physical emulation environment is being constructed using SCEPTRE™ and a real-time digital simulator RTDS. SCEPTRE™ enables implementation of different ICS communication protocols such as DNP3 and Modbus. Presently, the WSCC 9-bus sytem, pictured on the lefthand side of Fig. 5, is modeled in the RTDS system; we are interested in collecting data from the power system at different sampling rates due to non-contingency (low-sampling) and contingency events (high-sampling). The RTDS is able to stream C37.118 data that is collected in virtual phasor data concentrator (PDC) database; this database is then tapped into by SCEPTRE™ to update changes to the communication network and ICS devices. The representative communication network, developed by the team, is shown on the righthand side of Fig. 5.

The cyber-physical emulation environment connection between the SCEPTRE™ platform and RTDS is cur-

Authorized licensed use limited to: Texas A M University. Downloaded on April 05,2024 at 20:15:36 UTC from IEEE Xplore. Restrictions apply.

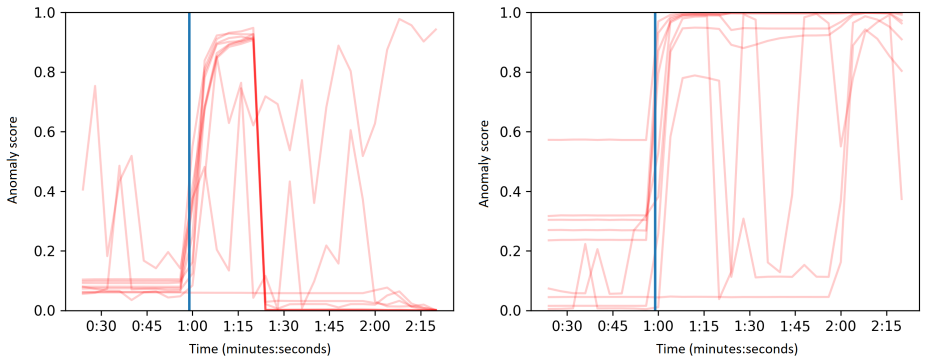

Fig. 4: Reported anomaly scores over time for the 10 test scenarios. A value of 1 indicates confidence in an anomaly and a value of 0 indicates the confidence of normal operations. Left: Cyber anomaly score. Right: Physical anomaly score.

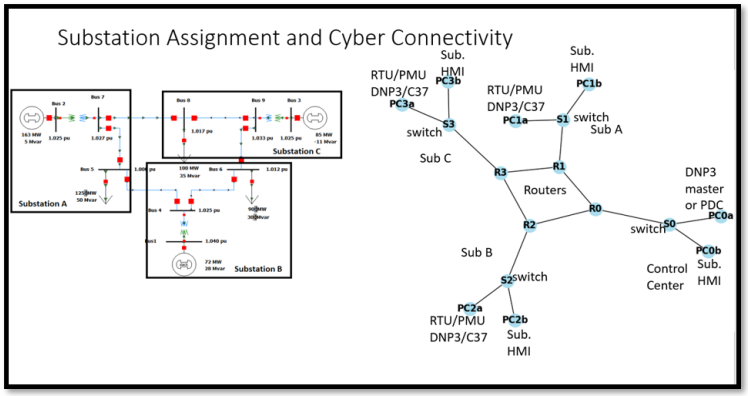

Fig. 5: WSCC 9-bus system oneline diagram and representative communication network with network devices such as remote terminal units (RTUs), phasor measurement units (PMUs), switches, etc.

rently being developed using the virtual phasor data concentrator (PDC) application. The overall integration plan is pictured in Fig. 6. The completed environment will enable modeling and testing of cyber-physical disturbances and the ability to extract high-fidelity data from both the cyber and physical systems. Furthermore, this data can be used to train and test the machine learning framework's ability to classify system conditions and deploy suitable cyber-physical corrective actions. We will also incorporate HIL equipment such as digital relays into the environment and test the next-generation relay voting scheme, as discussed in the next section.

VI. Next-Generation Relay Voting Schemes

To achieve selectivity and security in the HARMONIE-SPS approach, we are developing a next-generation relay voting scheme leveraging consensus algorithms. The proposed algorithm, shown in Fig. 7, extends traditional 2-out-of-3 voting schemes to a distributed system and aims to achieve consensus on system state and voting on response actions. Furthermore, the distributed computation prevents common failures from centralized failure points. Full details on the algorithm and the initial results using a simple simulation case study focusing on load shedding decisions can be found in [22].

To further develop this algorithm, we are presently testing it with the WSCC 9-bus system and will implement the consensus algorithms in the cyber-physical emulation environment using both virtual and HIL digital relays with the RTDS system. We will extend the focus from load shedding to a variety of corrective actions (both cyber and physical) and examine performance under different cyber-physical disturbances.

VII. Conclusions and Future Work

In this paper, the HARMONIE-SPS approach to achieve an adaptive, cyber-physical SPS implementation was presented; specifically, the machine learning framework for classifying system conditions, the automated corrective action assignment, next-generation relay voting scheme, and cyber-physical emulation en-

Authorized licensed use limited to: Texas A M University. Downloaded on April 05,2024 at 20:15:36 UTC from IEEE Xplore. Restrictions apply.

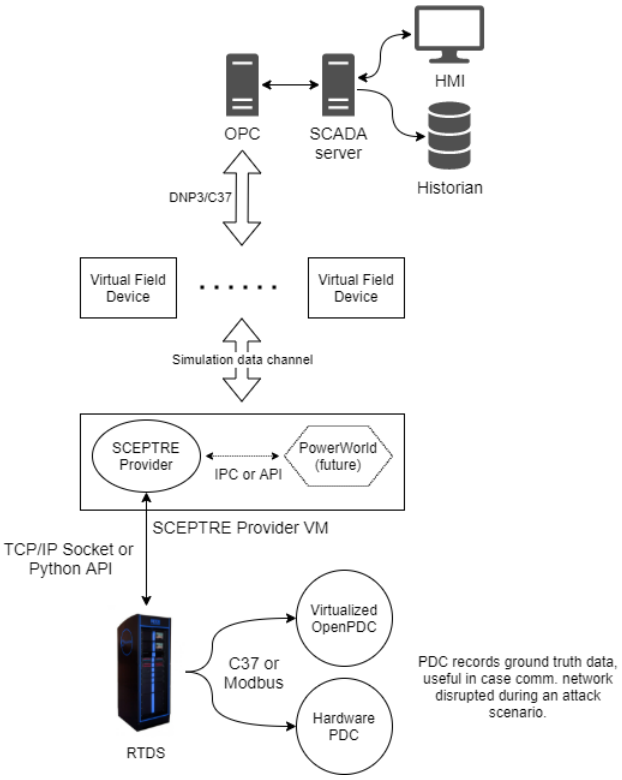

Fig. 6: Overall HARMONIE-SPS emulation environment architecture including SCEPTRE^{TM}, RTDS, and both virtualized and HIL components.

Algorithm 1 Relay voting with BFT

1) Relay i detects under frequency conditions
2) Relay i initiates request
3) Request for voting multicast to all other relays
4) All relays compute protection scheme calculations, determine load to shed
5) Each relay multicasts result to all other relays in group
6) Each relay waits for $f + 1$ replies, saves result.
7) Relay j that needs to shed load acts accordingly

Fig. 7: HARMONIE-SPS next-generation relay voting scheme algorithm for example load shedding application, from [22].

vironment initial results and next steps were shared. These initial results indicated promising HARMONIE-SPS performance for identifying cyber-physical disturbances and deploying suitable corrective actions with the prioritization of speed, selectivity, and/or security. The different components of HARMONIE-SPS will be cohesively deployed for an automated implementation; this deployment is will continue to be developed and tested under a variety of disturbance scenarios within the emulation environment.

ACKNOWLEDGMENTS

The authors would like to thank consultants to the project, Jason Stamp and Matthew Reno at Sandia National Laboratories and the Public Service Company of New Mexico, for their indispensable help and advice for this work.

REFERENCES

[1] K. Hemsley and R. Fisher, "History of industrial control system cyber incidents," Idaho National Laboratory, Tech. Rep., 2018.
[2] "Framework for improving critical infrastructure cybersecurity," National Institute of Standards and Technology, Tech. Rep., 2018.
[3] 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.
[4] "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, 2016.
[5] C. Lai, N. Jacobs, S. Hossain-McKenzie, P. Cordeiro, O. Onunkwo, J. Johnson, "Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators," Sandia National Laboratories, Sandia Report SAND2017-13113, Dec. 2017.
[6] Western Electricity Coordinating Council (WECC), "Remedial Action Scheme Design Guide," 2011.
[7] P. Anderson and B. LeReverend, "Industry experience with special protection schemes," *IEEE Transactions on Power Systems*, vol. 11, no. 3, pp. 1166–1179, 1996.
[8] J. G. O'Brien, E. L. Barrett, X. Fan, R. Diao, R. Huang, and Q. Huang, "Survey on RAS/SPS modeling practice," Pacific Northwest National Lab.(PNNL), Richland, WA (United States), Tech. Rep., 2017.
[9] M. D. Maram and N. Amjady, "Event-based remedial action scheme against super-component contingencies to avert frequency and voltage instabilities," *IET Generation, Transmission & Distribution*, vol. 8, no. 9, pp. 1591–1603, 2014.
[10] S. Wang and G. Rodriguez, "Smart RAS (Remedial Action Scheme)," in *2010 Innovative Smart Grid Technologies (ISGT)*. IEEE, 2010, pp. 1–6.
[11] Y. Zhang and K. Tomsovic, "Adaptive remedial action scheme based on transient energy analysis," in *IEEE PES Power Systems Conference and Exposition, 2004.* IEEE, 2004, pp. 925–931.
[12] H. Atighechi, P. Hu, J. Lu, G. Wang, and S. Ebrahimi, "A fast load shedding remedial action scheme using real-time data for bc hydro system," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE, 2016, pp. 1–5.
[13] X. Fan, R. Huang, Q. Huang, X. Li, E. L. Barrett, J. G. O'Brien, Z. Hou, H. Ren, S. Kincic, and H. Zhang, "Adaptive ras/sps system setting for improving grid reliability and asset utilization through predictive simulation and controls: A use case for transformative remedial action scheme tool (trast): Jim bridger ras evaluation and analysis," Pacific Northwest National Lab.(PNNL), Richland, WA (United States), Tech. Rep., 2019.
[14] S. Hossain-McKenzie, K. Davis, M. Kazerooni, S. Etigowni, S. Zonouz, "Distributed controller role and interaction discovery," in *2017 19th International Conference on Intelligent System Application to Power Systems (ISAP), San Antonio*, 2017.
[15] S. Hossain-McKenzie, "Protecting the power grid: strategies against distributed controller compromise," Ph.D. dissertation, University of Illinois Urbana-Champaign, 2017.
[16] S. Boyd, N. Parikh, C. Chu, B. Peleato, J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Foundations and Trends in Machine Learning*, 2011.
[17] The MITRE Corporation, "ATT&CK," 2020. [Online]. Available: https://attack.mitre.org/

Authorized licensed use limited to: Texas A M University. Downloaded on April 05,2024 at 20:15:36 UTC from IEEE Xplore. Restrictions apply.

[18] A. Sahu, P. Wlazlo, Z. Mao, H. Huang, A. Goulart, K. Davis, and S. Zonouz, "Design and evaluation of a cyber-physical testbed for improving attack resilience of power systems," *IET Cyber-Physical Systems: Theory & Applications*, vol. n/a, no. n/a. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/cps2.12018

[19] 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.

[20] 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.

[21] *WSCC 9-Bus System*, Online, Illinois Center for a Smarter Electric Grid, 2021.

[22] 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.

Authorized licensed use limited to: Texas A M University. Downloaded on April 05,2024 at 20:15:36 UTC from IEEE Xplore. Restrictions apply.