Cyber-Physical Events Emulation Based Transmission and Distribution Co-Simulation for Situation Awareness and Grid Anomaly (SAGA) Detection

Preprint

Xin Fang, Mengmeng Cai, and Anthony Florita

National Renewable Energy Laboratory

Presented at the 2021 IEEE Power & Energy Society General Meeting
July 25–29, 2021

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5D00-78189
July 2021

Cyber-Physical Events Emulation Based Transmission and Distribution Co-Simulation for Situation Awareness and Grid Anomaly (SAGA) Detection

Preprint

Xin Fang, Mengmeng Cai, and Anthony Florita

National Renewable Energy Laboratory

Suggested Citation
Fang, Xin, Mengmeng Cai, and Anthony Florita. 2021. *Cyber-Physical Events Emulation Based Transmission and Distribution Co-Simulation for Situation Awareness and Grid Anomaly (SAGA) Detection: Preprint*. Golden, CO: National Renewable Energy Laboratory. NREL/CP-5D00-78189. https://www.nrel.gov/docs/fy21osti/78189.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5D00-78189
July 2021

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER). The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

U.S. Department of Energy (DOE) reports produced after 1991 and a growing number of pre-1991 documents are available free via www.OSTI.gov.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

NREL prints on paper that contains recycled content.

Co-simulation software for Cyber-Physical systems
SAGA - Situational Awareness of Grid Anomalies

Cyber-Physical Event Emulation-Based Transmission-and-Distribution Co-simulation for Situational Awareness of Grid Anomalies (SAGA)

Xin Fang, Mengmeng Cai, Anthony Florita
Power Systems Engineering Center
National Renewable Energy Laboratory
Golden, CO, USA
{Xin.Fang, Mengmeng.Cai, Anthony.Florita}@nrel.gov

***Abstract*—Energy management of transmission and distribution networks (T&D) is becoming more challenging with the accelerated adoption of distributed energy resources (DERs)—such as distributed photovoltaic generation and battery energy storage systems (BESS)—on the electric grid. To better analyze the impacts of DERs on both transmission and distribution systems, a comprehensive T&D co-simulation platform is developed. Further, with DERs more actively participating in system operation—e.g., by providing real-time grid services—their cyber vulnerability needs to be better understood to maintain system reliability. This paper discusses a cyber-physical events emulation-based T&D co-simulation platform to perform comprehensive cyber events emulations, physical simulation, and analysis of interdependent impacts. Results from the case studies—which show how cyber events on a synthetic distribution network can impact operations on the transmission and distribution network—validate that the proposed T&D co-simulation platform can perform cyber-physical events emulation and produce response in near realtime; therefore, with extensive simulation using the proposed co-simulation platform, the system operators can accumulate adequate training data for system situational awareness of grid anomalies.**

***Index Terms*—Cyber-physical system, transmission-and-distribution co-simulation, situational awareness, anomalies detection.**

I. Introduction

With the substantially increasing penetration levels of distributed energy resources (DERs) (such as distributed photovoltaic [PV] generation and battery energy storage) in power systems, DERs are impacting not only distribution system operation (such as the local voltage profile) but also transmission system operation (such as generation scheduling and reserve procurement) and bulk power system stability [1]. Meanwhile, with the increasing capacity of DERs, DERs are being used to more actively participate in system ancillary services coordination and reserves provision to increase operational flexibility and explore additional revenue [2]. FERC Order 2222 [3] states that the electricity markets in the United States should remove all barriers preventing DERs from participating in their markets; therefore, DERs will continue to increase their participation in future system and market operation. When DERs are actively communicating with aggregators and operators to provide real-time services, such as frequency regulation, they are vulnerable to various cyber-physical events, such as false data injection, denial of service, device hijacking, and communications network congestion [4]–[6]. To comprehensively analyze the impacts of cyber-physical events and mitigate those that target DERs on both transmission and distribution (T&D) system operation, an advanced system situational awareness and grid anomalies detection model needs to be developed. To achieve this goal, a cyber-physical event embedded T&D co-simulation platform is developed to simulate large amounts of the system offline operation data while considering various cyber-physical events. This co-simulation platform can act like a “digital-twin” of the actual system to emulate the cyber-physical events. With this platform, the operators can analyze the actual response of cyber-physical events in the physical system to understand the mechanism behind them.

Recently, T&D co-simulation has attracted increasing attention because of the substantial increase of DERs. In most T&D co-simulation studies [7], the focus has been on steady-state T&D networks power flow simulation to obtain the T&D voltage profile and to ensure that the local voltage can be improved with advanced DERs control. In [8], the authors developed an integrated T&D framework to simulate the impacts of DERs on T&D system steady-state operation. A dynamic co-simulation framework for T&D systems was introduced in [9]. In these T&D studies, however, the cyber layer or the impacts of potential cyber-physical events were not well modeled; therefore, making it hard to capture system situational awareness and grid anomalies detection from potential cyber-physical perspective. With more DERs integrated into power systems, it is urgent to have a T&D co-simulation platform to simulate the impacts of potential cyber-physical events in distribution on T&D operation.

This work was authored by Alliance for Sustainable Energy, LLC, the Manager and Operator of the National Renewable Energy Laboratory for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergence Response (CESER). The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

To study the impacts of cyber-physical events on T&D system operation, such T&D co-simulation also needs to include a cyber-physical events emulation module that captures the interactions between the cyber layer and the DERs in the distribution network, especially in the distribution network. The Hierarchical Engine for Large-scale Infrastructure Co-Simulation (HELICS) [10], provides a modular framework for transmission-distribution-communication (cyber-physical) simulation, but its built-in and existing external tools for cyber simulation do not readily support the more sophisticated models needed to improve system situational awareness and grid anomalies (SAGA) detection. To fill this research gap, this paper introduces a cyber-physical events emulation-based T&D co-simulation platform. A comprehensive cyber-physical events emulation module will be introduced to model the impacts of potential cyber events on the distribution system. Then, through the T&D co-simulation platform, the impacts of the cyber-physical events on the T&D network will be studied. Note that the proposed framework is modularized and extensible such that the communication layer can be added in the future to emulate the communication latency [11] and potential cybersecurity issues. The modular and large-scale co-simulation capability of HELICS will be leveraged in the next phase large-scale system testing.

The rest of this paper is organized as follows. Section II introduces the overall framework of the proposed cyber-physical events emulation-based T&D co-simulation platform. Section III introduces the cyber-physical events emulation model to consider different types of potential cyber-physical events in the distribution network. Section IV performs the case studies to analyze the impacts of various cyber-physical events on T&D system operation. Section V concludes the paper.

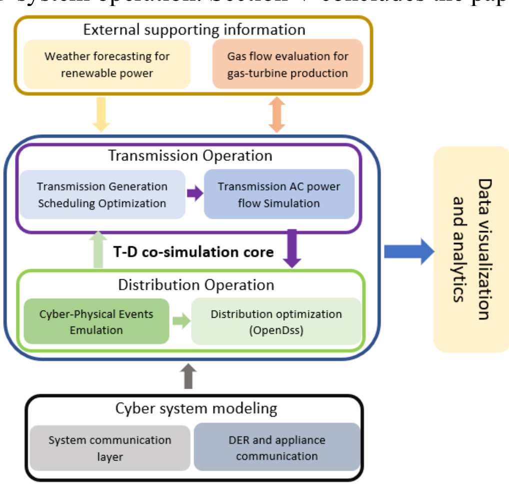

Fig. 1. The framework of SAGA

II. Cyber-Physical Event Emulation-Based T&D Co-Simulation

The proposed SAGA platform is depicted in Fig. 2. SAGA includes four major components: an external forecasting model for renewable power and other supporting information forecasting, a T&D co-simulation core for T&D optimization, a cyber system modeling for the DERs and appliance communications, and the data visualization and analytics. With different energy systems, such as electricity and natural gas networks, being increasingly interconnected because of the increasing renewable energy integration and increasing gas-fired units, electricity system situational awareness should be extended to include external system information, such as renewable energy forecasting and natural gas network monitoring, as shown in the first component. For machine learning and ease of operation, the SAGA real-time simulation results data should be visualized and stored in a specified location, such as the machine learning grid anomalies detection training database, which is shown in the data visualization and analytics component. A real-time distribution voltage measurement data from cable TV data will also be integrated in the data analytics module to training the simulated data with actual measurement data. In addition, the communications layer can be comprehensively modeled in the cyber system modeling component to capture the communication latency and cyber impacts.

This paper focuses on the introduction of cyber-physical events emulation into distribution networks and the multi-timescale operation in the transmission network considering the impacts of potential cyber-physical events.

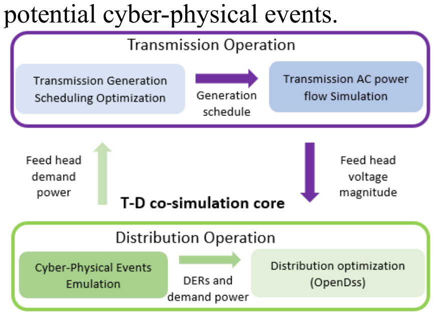

Fig. 3. Information exchanges between T&D co-simulation modules

The T&D co-simulation core includes four submodules: a transmission generation scheduling optimization, a transmission AC power flow simulation, a distribution power flow optimization, and a cyber-physical events emulation. The transmission generation scheduling optimization is to decide the multi-timescale system generation scheduling, including the day-ahead unit commitment, the day-ahead economic dispatch, the real-time unit commitment, and the real-time economic dispatch. Because the transmission generation scheduling optimization is based on DC optimal power flow models, the transmission AC power flow simulation is used to obtain a feasible AC power flow solution with the generation outputs from the generation scheduling optimization module. The ANDES package, developed by UTK, will be used to obtain the transmission system AC power flow [12]. Then the voltage magnitudes of the transmission buses are sent to the distribution power flow simulation model. The distribution optimization is used to obtain the distribution network power flow considering the feeder-head voltage magnitude exchange with the transmission system. Then the updated distribution system demand considering the distribution network power losses is sent to the transmission generation scheduling model to update the system generation profile. The OpenDSSDirect package is used for the distribution network power flow simulation [13]. The cyber-physical events emulation is used to obtain the distribution network demand and DER generation profiles under different cyber-physical events. The generation scheduling optimization and the cyber-physical event emulation packages are developed under two ongoing projects and will be publicly released after the projects end. All four models are developed in the Python environment; therefore, they can be integrated into the same simulation platform. The information exchanges between different modules are shown in the Fig. 4.

III. CYBER-PHYSICAL EVENT EMULATION

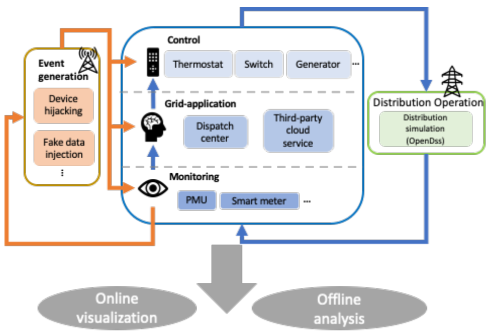

Fig. 5. Cyber-physical event emulation framework

As illustrated in Fig. 6, the cyber-physical events emulation module consists of four layers. DER (e.g., battery storage, distributed generator, thermostatic-controlled loads) modeling is implemented at the *control* layer. It interacts with the OpenDSS model in the form of nodal power injections/withdraws. The *monitoring* layer models the process of sensor allocation, time-stamp labeling, and data collection. Its interface with the OpenDSS model is configurable with respect to the system observability to support the cyber-physical events emulation under various observability assumptions. The *grid-application* layer acts as either the dispatch center managed by the distribution system operator or the cloud service center managed by third-party DER manufacturers given different application scenarios. It integrates applications that target improving system reliability and efficiency through actively coordinating groups of DERs. Examples of these applications include economic dispatch, voltage regulation, and demand response. Finally, the *event generation* layer plays the key role in designing logics behind the events based on different attack techniques. It injects malicious command/data into the *control*, *monitoring*, and *grid-application* layers once an event instance is triggered, which causes undesirable disruptions to normal system operation.

Jointly, the *control*, *monitoring*, and *grid-application* layers form a closed control loop on top of the OpenDSS model, turning the passive distribution network into a proactive one. The *event generation* layer is exposed to different links inside the closed control loop, enabling SAGA to emulate events with diversified attack access points. Another configurable property of SAGA is reflected by the path from the *monitoring* layer to the *event generation* layer (see Fig. 3). Different assumptions about accessibility to the measurement data can be made to simulate events with different levels of system knowledge. Given that cyber-physical events usually lead to unsecured operation conditions or increase operation cost, simulation results will be sent to a visualization engine and subsequently an analysis engine to support online visualization and offline analysis on the economic and stability consequences.

Above all, with this cyber-physical events emulation model, SAGA can provide a cyber-physical event emulation testbed modeled in a bottom-up fashion in the vision of the future decentralized and proactive smart grid. The diversified events emulation capability distinguishes SAGA from existing efforts. Different components inside the event emulation module are developed in a modularized fashion to facilitate its integration with the T&D core and furture extension.

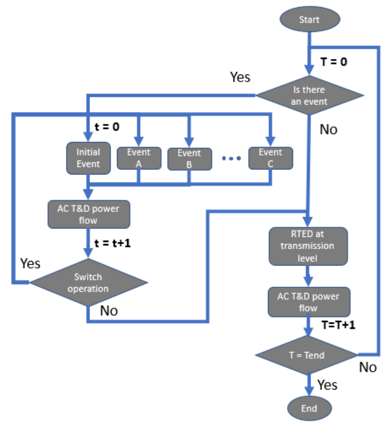

Fig. 7. The simulation flow of cyber-event emulation in the T&D co-simulation

In the real-time operation, the system generation scheduling and AC power flow will be run every 5 minutes. Then the distribution power flow will be simulated to consider whether there is a cyber-physical event in the distribution system. The simulation flow and the interaction among different modules are depicted in Fig. 8.

IV. CASE STUDIES

This section tests the proposed model in an 18-bus transmission system and a synthetic distribution network (Austin area, TX). The impacts of different cyber-physical events on T&D network operation will be analyzed. All simulations are performed in a Python-based scheduling tool on a personal laptop with Intel Core i5 as the central processing unit.

A. *T&D Test System*

The transmission test system is from the 18-bus system depicted in Fig. 5. Detailed system data can be found in [14]. The test distribution system is shown in Fig. 6. The active and reactive power profile of the distribution network is depicted in Fig. 7. The distribution feeder is connected to Bus 2 in the transmission system. To study the impacts of distribution cyber-physical events on system operation—such as transmission system operation cost, transmission system load, and distribution network voltage—different cyber-physical events are simulated and compared to the base case without any cyber events. Three different cyber-physical events are simulated, as listed below. In Case 2 to Case 4, the cyber-physical events happen at 12 p.m. and are cleared at 1 p.m. that day; therefore, the cyber-physical event duration for each case is 1 hour.

Case 1: Base case without any cyber-physical events

Case 2: Distribution load perturbed with a factor of 1.5 in the distribution network

Case 3: One single-line-to-ground fault happened in the distribution network.

Case 4: One switch in the distribution network is opened.

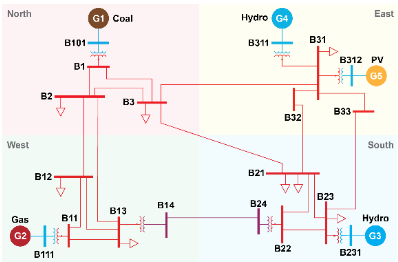

Fig. 5. 18-bus transmission test system

Fig. 6. Distribution network topology

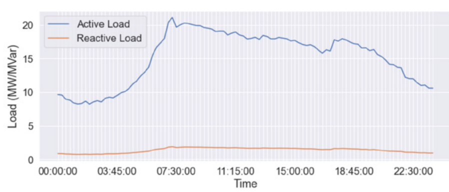

Fig. 7. Active and reactive load profile of the distribution network

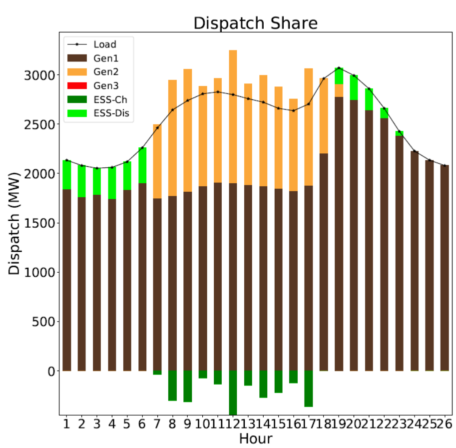

Fig. 8. Day-ahead generation dispatch in the base case

B. *Impacts of Cyber-Physical Events on Transmission Network*

The generation dispatch in the base case is shown in Fig. 8. The load curve, the load differences, and the generation cost difference between the cyber-physical events and the base case are shown in Fig. 9 to Fig. 10.

Fig. 9 and Fig. 10 demonstrate that different cyber-physical events in the distribution network have various impacts on the transmission load and consequently have different generation cost curves, as shown in Fig. 11. The load-perturbed events and the single-line-to-ground faults in the distribution network have a higher impact on the transmission network than the single switch open event.

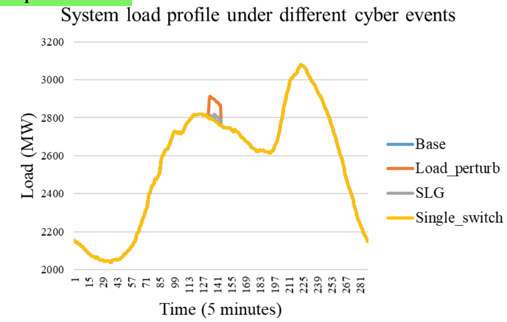

Fig. 9. Transmission load curves in different cyber-physical events

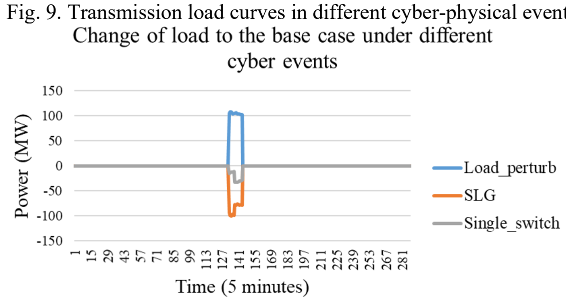

Fig. 10. Load differences between cyber-physical cases and base case

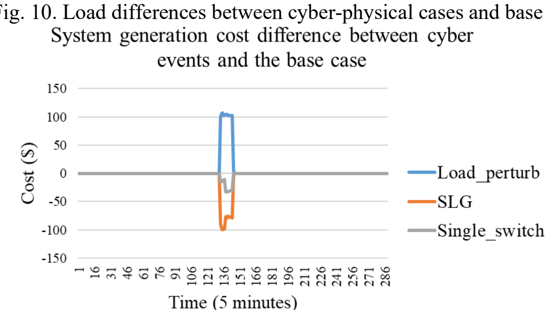

Fig. 11. System generation cost differences between cyber-physical cases and base case

C. *Impacts of Cyber-Physical Events on Distribution Network*

The distribution network buses' average voltage magnitude and the voltage differences between the cyber-physical events and the base case are depicted in Fig. 12 and Fig. 13.

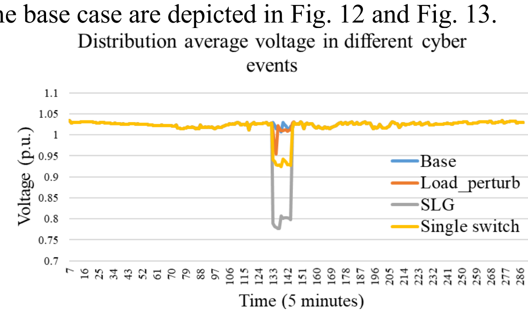

Fig. 12. Distribution average voltage in different cases

Fig. 12 and 13 also demonstrate that the load-perturbed events and the single-line-to-ground faults in the distribution network have a higher impact on the distribution voltage profile than the single switch open event; therefore, in T&D system operation, the operators should be better prepared for these cyber-physical events. The line grounding faults can lead to low voltage in the distribution network. This voltage violations can also be observed from the real time cable TV voltage measurement data which validate the accuracy of the proposed co-simulation framework.

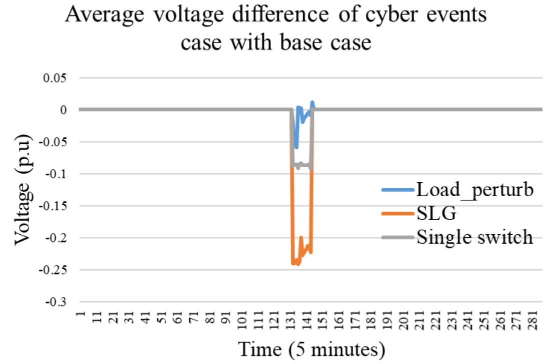

Fig. 13. Feeder-head voltage differences between the cyber cases and the base case

D. *Sensitivity of Distribution Load Perturbation*

The sensitivity of the load perturbed in the distribution network is studied in this subsection. Fig. 14 and Fig. 15 show the voltage profiles and generation cost curves under different levels of load perturbation.

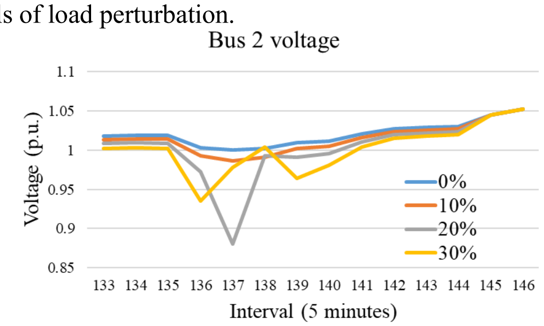

Fig. 14. Feeder-head voltage under different levels of load perturbation

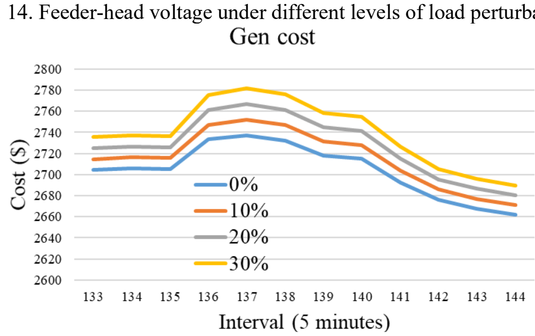

Fig. 15. Generation cost under different levels of load perturbation

The impacts of the load perturbation on both the distribution network voltage profile and transmission generation cost are clearly depicted. The higher the load is perturbed, the larger the voltage and generation cost will be changed.

V. Conclusions

This paper presented a cyber-physical events emulation-based T&D co-simulation platform to study the impacts of various cyber-physical events on T&D system operation. A detailed cyber-physical event emulation model is introduced. With the proposed platform, various cyber-physical events can be simulated, and their impacts on T&D network operation can be captured; therefore, with extensive simulation using this platform, system operators can accumulate necessary data sets for strengthening the system situational awareness and grid anomalies detection capability. Case studies concerning different kinds of cyber-physical events demonstrated that the local cyber-physical events in the distribution network can not only impact the local distribution network voltage profile but also change the transmission operating cost and the transmission voltage profile. The significance of the cyber-physical events is different, which means that system operators should pay different levels of attention to various cyber-physical events. The load perturbation and line-to-ground faults have high impacts on T&D operation. More extensive studies about how to detect and mitigate these kinds of cyber-physical events will be the subject of our future work. Including a communication layer to emulate the communication latency and potential cyber issues will also be our future work.

References

[1] X. Zhou, Z. Liu, C. Zhao, and L. Chen, "Accelerated Voltage Regulation in Multi-Phase Distribution Networks Based on Hierarchical Distributed Algorithm," *IEEE Trans. Power Syst.*, pp. 1–1, Oct. 2019.

[2] S. van der Stelt, T. AlSkaif, and W. van Sark, "Techno-economic analysis of household and community energy storage for residential prosumers with smart appliances," *Appl. Energy*, vol. 209, pp. 266–276, 2018.

[3] C. Cano, "FERC Order No. 2222: A New Day for Distributed Energy Resources," 2020.

[4] Y. Zhang, L. Wang, and Y. Xiang, "Power System Reliability Analysis with Intrusion Tolerance in SCADA Systems," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 669–683, Mar. 2016.

[5] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in Distributed Power Systems," *Proc. IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017.

[6] C. W. Ten, G. Manimaran, and C. C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," in *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans*, 2010, vol. 40, no. 4, pp. 853–865.

[7] M. Caramanis, E. Ntakou, W. W. Hogan, A. Chakrabortty, and J. Schoene, "Co-optimization of power and reserves in dynamic T&D power markets with nondispatchable renewable generation and distributed energy resources," *Proc. IEEE*, vol. 104, no. 4, pp. 807–836, Apr. 2016.

[8] B. Palmintier *et al.*, "IGMS: An Integrated ISO-To-Appliance Scale Grid Modeling System," *IEEE Trans. Smart Grid*, vol. 8, no. 3, May 2017.

[9] R. Huang, R. Fan, J. Daily, A. Fisher, and J. Fuller, "Open-source framework for power system transmission and distribution dynamics co-simulation," *IET Gener. Transm. Distrib.*, vol. 11, no. 12, Aug. 2017.

[10] B. Palmintier, D. Krishnamurthy, P. Top, S. Smith, J. Daily, and J. Fuller, "Design of the HELICS high-performance transmission-distribution-communication-market go-simulation framework," in *2017 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2017 - Held as part of CPS Week, Proceedings*, 2017.

[11] J. Zhang, A. Hasandka, S. M. S. Alam, T. Elgindy, A. R. Florita, and B. M. Hodge, "Analysis of Hybrid Smart Grid Communication Network Designs for Distributed Energy Resources Coordination," in *2019 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2019*, 2019.

[12] H. Cui and F. Li, "ANDES: A Python-Based Cyber-Physical Power System Simulation Tool," in *NAPS 2018*, 2019.

[13] "opendssdirect package — OpenDSSDirect.py 0.5.0 documentation." [Online]. Available: http://dss-extensions.org/OpenDSSDirect.py/opendssdirect.html#module-opendssdirect.LoadShape. [Accessed: 12-Oct-2020].

[14] Q. Wang, W. Hongyu, T. Jin, B. M. Hodge, W. Li, and C. Luo, "Analyzing the impacts of increased wind power on generation Revenue Sufficiency," in *IEEE PESGM*, 2016, vol. 2016-Novem, pp. 1–5.