IEEE TRANSACTIONS ON
INDUSTRY
APPLICATIONS
A PUBLICATION OF THE IEEE INDUSTRY APPLICATIONS SOCIETY
WWW.IEEE.ORG/IAS

A Real-Time Federated Cyber-Transmission-Distribution Testbed Architecture for the Resiliency Analysis

V. Venkataramanan, *Member, IEEE,* Partha S. Sarker, *Student Member, IEEE,* K. S. Sajan, A. Srivastava, *Senior Member, IEEE*, and A. Hahn, *Member, IEEE*

***Abstract*—With the ongoing automation driven by the push towards the smart electric grid and the advancement in associated cyber infrastructure, the interaction between physical (electric transmission and distribution (T&D) systems), cyber (communication, automation, and control) and human (grid operators and decision-makers) is increasingly becoming more complex. This creates the requirement of analyzing the effect of the transmission system on the distribution system and vice-versa with consideration of the additional complexity of the cyber infrastructure. Such an integrated testbed will also help with resiliency analysis, where resiliency refers to the ability of the system to continue serving energy to the critical loads even with limited extreme contingencies. Interaction of the physical power grid with the cyber layer can be effectively modeled using real-time (RT) simulator for developing and validating various operational and control algorithms. Testbeds using RT simulators with multiple capabilities have been developed at different institutions. Still, no single existing testbed can offer full scalability while simultaneously meeting high fidelity requirements for resiliency experimentation. Co-simulating federated testbed assets can provide a scalable experimentation platform that can be leveraged for verification and validation. In this paper, an architecture is developed for federated cyber-physical testbed. A local federation with two real-time simulators is developed: Real-Time Digital Simulator (RTDS) and OPAL-RT have been interfaced using VILLAS framework for end-to-end testing. Also, a real-time linear predictor is developed and integrated here to address the communication latency impact on geographically allocated federated RT simulation. Lastly, resiliency analysis tools are formulated and utilized for T&D systems. As an illustrative use case, the resiliency of a T&D test system is simulated, and the results are analyzed. A 179 bus WECC transmission system is developed using OPAL-RT/ HYPERSIM, and a modified IEEE 13 node feeder system is modeled in RTDS/ RSCAD and interfaced for resiliency analysis.**

I. Introduction

With enhanced digitalization and automation leading to an active distribution system, traditional analysis for T&D systems being in silos are becoming ineffective. Co-simulation of T&D system is becoming more important with the proliferation of control and automation in the distribution grid, and increasing stress in the transmission grid [1]. Testbeds allow us to test newly developed control algorithms [2] in a safe and controlled environment considering the 'system of systems' concept. The testbed can be regarded as an intermediate step between theoretical validation and practical field implementation. It is hard for researchers and industrial practitioners to test new methods and technologies in the field, especially in critical infrastructure such as the power grid. The testbed allows a safe laboratory environment capable of emulating the actual field while still providing more fidelity and accuracy than computer simulations or table-top experiments.

Interaction between transmission and distribution systems becomes essential to understand the systems behaviour in terms of resiliency. Resiliency definitions for power systems are still evolving and there is no related standard or guidelines. Authors in [3] have considered a combined transmission-distribution system resiliency formulation. Authors in [4]–[6] have considered formulated resiliency with a different focus based on distribution system performance. In this work, the resiliency of the power grid is defined as the ability of the system to supply critical load even during and after extreme events. In the transmission system, few critical loads are considered to be present at all of the substations, while individual critical loads are identified in the distribution system. This definition is in line from the recent Department of Energy (DoE) publication on the definition of resilience [7]. Transmission system analysis is usually performed by lumping the distribution system as a single load. At the same time, this assumption is valid in most cases, but not adequate for resiliency analysis as it fails to consider if power is supplied to the critical loads. Similarly, for distribution systems, the point of interconnection to the transmission grid is modeled as an infinite source, which might not be valid for resiliency studies. Furthermore, digital control devices are being used to control many physical power system components. An attacker can remotely control a relay through cyber-attack and can create events like Aurora Vulnerability [8]. On the other hand, attacker can physically damage a sensor, which can lead to misleading information and cause malfunction of certain digital control devices. Besides these, there are many interdependencies between the physical and

Partha S. Sarker, Sajan K. S., A. Srivastava and A. Hahn are with the Washington State University, Pullman, WA 99163 USA. (E-mail: anurag.k.srivastava@wsu.edu)

V. Venkataramanan graduated from the Washington State University and now working at the Massachusetts Institute of Technology (MIT).

This material is partially based upon work supported by the Department of Energy under Award Number DE-OE0000780 and the National Science Foundation FW-HTF Award #1840192. We would like to thank Dr. S. Chanda and Dr. Tushar for their technical contributions. We would also like to acknowledge RWTH Aachen University, Germany for the VILLAS Framework.

Digital Object Identifier 10.1109/TIA.2020.3023669

cyber layers of a power system [6] requiring analysis using cyber-transmission-distribution testbed. The co-simulation of transmission and distribution systems, along with cyber components, is performed to address the above mentioned problems. The data from these simulations are used to compute the resiliency that covers both cyber and physical layers of the power system. The resiliency computation exchanges data between T&D system, and the resiliency scores with and without T&D co-simulation are compared for the distribution system.

Decades of efforts are needed to first co-simulate physical systems, integrate cyber systems, and then human factor aspects for needed cyber-physical-human analysis. Co-simulation of transmission and distribution system is essential to understand the holistic system-wide performance and one of the first steps towards the larger effort. In many cases, a single simulation package or simulator is incapable of co-simulating the transmission and distribution systems, especially at near real-time speeds [9]. The solution for the issue, as mentioned earlier, is to have federated testbed. Federation is the concept of leveraging distributed assets to create a unified test environment for simulating various scenarios. In order to perform large-scale power grid experimentation and leverage investment on testbed hardware from different educational research centers, national laboratories, and the industries, it is desirable to combine geographically distributed resources for energy systems research [10].

There are a limited number of previous efforts, outlining real-time simulation using federated testbed [11], [12], [13] and [14]. Even though the federated RT simulation has numerous benefits, there are some main challenges, such as: 1) power system partitioning; 2) time synchronization between different simulators; and, 3) satisfying dependability of communication between the partitioned systems, for example, data loss, communication latency etc [15].

An established method for co-simulating various simulators, including real-time simulators are the virtually interconnected laboratories for large systems simulation/ emulation (VILLAS) platform [16]. It has various components, including a VILLAS node. The VILLAS node operates as a client-server management application that processes and manages the data to interface different simulators. In our previous work [17], a testbed architecture has been developed for transmission-distribution co-simulation using real-time simulators. VILLAS node is used to interface the RTDS and the OPAL-RT and manage the co-simulation. Hypersim is used as the modeling and simulation interface for OPAL-RT, and extension of the VILLAS node has been done here for connecting to this software. One of the important features of the proposed architecture is that it can work even if one of these RT simulators is swapped with another one, and the focus of this work is on interfacing architecture and federated facility. Our work is one of the first to put together cyber, transmission and distribution system simulators in real-time for "complete system resilience analysis". The main contributions of this paper can be summarized as:

1) To propose a novel method to quantify the cyber-physical resiliency of integrated transmission and distribution system. Developed testbed will: a) be accessible to other researchers for integrated real time simulation, b) offer integration mechanisms to replace proposed simulators in any domain (transmission, distribution and cyber) by simulator/ emulator proposed by other researcher/ industry for specific application validation, c) be interfaced with blackbox validation using remote federated testbed architecture, specifically useful for defense applications.
2) To develop a transmission-distribution co-simulation testbed architecture using specific example simulators: RTDS and OPAL-RT for validating the proposed approach. Developed architecture offers flexibility to replace one simulator with another considering data delays and synchronization to interface different simulators/ emulators over geographical distance.
3) Analyzing the effect of communication latency in geographically distributed real-time federated simulators/emulators using linear estimation. Additionally, a new User Coded Module (UCM) is created in the Hypersim for communicating the data in the Hypersim simulation to the VILLAS node. This module creates a socket connection from the Hypersim computer to the real-time simulator, and then subscribes to the parameters required by the user to facilitate interfacing different simulators.
4) Validation of developed federated testbed for multiple resiliency test cases, which can be extended for other applications. Testbed facilitates analysis for data exchange needed between different stakeholders to enable power grid resilience.

II. Federated Co-simulation Testbed

Various testbeds exist which use ad-hoc approaches for interfacing simulators, which are often constrained to certain experiments and security tools [30], [31]. Table I highlights the differences through a detailed comparison of several testbeds. These approaches offer the flexibility of choosing the granularity in models, and also offers more choices for the interface. The downside is that these testbeds might often be application-specific and might need to be validated. Since the ad-hoc method does not require an external simulation framework or controller, these testbeds might often be faster and accurate for the particular application. The authors have developed such specific testbeds as detailed in [17], [32]–[34]. In [17], a microgrid cyber-physical testbed is developed that is focused on security research. A reconfiguration algorithm is used as the control application, and the effects of cyber-attacks on the performance of reconfiguration are studied. Other interfaces include simulation of transmission systems, custom developed middleware, and data delivery mechanisms in [35] using similar approaches. The work reported in [34] uses real-time simulators, including RTDS and OPAL-RT, a custom developed communication simulator ISERINK, and

TABLE I
TESTBEDS FOR CYBER-PHYSICAL ANALYSIS

Testbed	Power System Simulator	Communication System Simulator	Scalability	Research Focus
GECO [18], Virginia Tech	PSLF	NS-2	Transmission level systems	PMU protection systems
EPOCHS [19], Virginia Tech	PSCAD	NS-2	Transmission level systems	Special protection systems (SPS)
VPST [20], UIUC	RTDS, PowerWorld, and other software	DeterLab, SDN Testbed	Transmission and Distribution systems	Various security thrusts including CyPSA, and PMU testing
Greenbench [21], NCSU	PSCAD	OMNET++	Microgrid and distribution systems	Data-driven cyber-attacks
GENI-Deter-WAMS [22], NCSU	RTDS	ExoGENI and Deter	Transmission systems	Various security applications, including wide area control
Mississippi State University [23]	RTDS	Hardware based	Small transmission level systems	Various cyber-attacks and data-driven analysis
CRUTIAL [24], CESI RICERCA	FPGA and Matlab for microgrid testbed	Hardware based	Hardware restricted	SCADA attacks, communication impact on inverter and microgrid control
VIKING [25], KTH	SCADA and EMS system	Hardware based	Transmission systems	Network based cyber attacks, attacks on smart grid algorithms
FNCS [26] framework, PNNL	GridLAB-D, PowerFlow	NS-3	Transmission and Distribution systems	Smart grid application test
HELICS [27] framework	PSST, MATPOWER, GridDyn, GridLAB-D	NS-3	Transmission and Distribution systems	Cyber-physical-energy co-simulation
ERIGrid [28]	OPAL-RT, MATLAB, SCADA, Power system hardware	Hardware based	Transmission and Distribution systems	Facilitates testing of smart grid solutions on system level considering cyber-physical-energy system in a holistic manner
WSU Educational Testbed [29]	DIgSILENT, PSCAD, GRIDLAB-D, MATLAB and RTDS	NS3	Distribution system	Educational modules for students to study the concepts cyber-distribution system through an integrated testbed
WSU Testbed [17]	OPAL-RT, RTDS	CORE, NS-3, and Mininet	Transmission and Distribution systems	Real-time cyber-physical resiliency analysis and testing resiliency based solutions with scalability to implement in both cyber and physical layer

interfaces various security tools in the testbed. Besides, there are other testbeds from national laboratories, such as [36] for cyber-physical analysis.

While the testbeds presented above have their advantages, they focus on simulating either the transmission or distribution system at a time. A detailed study of the effect of transmission on distribution and vice versa in terms of Electromagnetic Transient Programs (EMTP) simulation lacks in most of the current testbeds. Furthermore, hardware present in most research institutions is also limited. Thus the scale of the experiments is bounded to small systems. Scaling up hardware at a single location will increase the cost exponentially. Federation of resources, in which resources at different institutions at different locations can be shared, presents a more feasible approach for large-scale experiments. The federated co-simulation testbed at Washington State University(WSU) is motivated towards enabling large-scale experimentation studying the interdependency between various systems such as power/physical systems and communication systems. The focus of the testbed at WSU is to study the resiliency of a combined transmission-distribution system. The WSU testbed can be configured in multiple ways depending on the simulation. In this paper, the microgrid cyber-physical security analysis capability has been demonstrated. The WSU testbed uses the following components:

1) RTDS and OPAL-RT for simulating the distribution and transmission system respectively,
2) CORE, NS-3, and Mininet for emulating the communication network,
3) VILLAS node for connecting simulators and data exchange, and
4) A resiliency based reconfiguration algorithm.

An overview of the components of the WSU testbed is shown in Fig. 1. Further details about the individual components can

be found in [17]. The interfacing of these components using the VILLAS node is briefly described as follows.

A. Real-Time Simulation Using RTDS

The power system model has been developed in RTDS, which offers the flexibility of connecting hardware components to the simulated power system. Also, the control algorithms used in the simulation can be validated to work in real-time. RTDS simulates the system with a time step of 50 μs [37]. RTDS has been previously used in various testbeds at WSU, and is now used to simulate the distribution system, and interfaced with the transmission system using VILLAS node. The main concept behind the interface between the power system simulator RTDS and external software can be considered as User Datagram Protocol (UDP/IP). RTDS's output is visualized in its RunTime screen. The RunTime is in the same machine in which the RSCAD is installed. The RunTime allows the user to use a scripting interface to provide commands in real-time. The VILLAS node receives the data from the simulation by opening a UDP connection with the RunTime interface and processes and communicates this data to the other simulator.

B. Real-Time Simulation Using OPAL-RT

HYPERSIM is the modeling interface for the real-time simulator OPAL-RT [38]. It has an extensive library for both power electronics and power systems. It provides an open, flexible, and scalable architecture and high-speed parallel processing that enables simulation at time steps of 5-200 μs. OPAL-RT has a suite of applications such as RT-LAB, ScopeView, and TestView that enable the user to monitor and control the simulation. The OPAL-RT allows data export in multiple formats, and this is used to send the data from the Hypersim to the VILLAS node.

C. VILLAS Framework

VILLAS [39] node is a gateway for exchanging data between federated real-time digital simulators. It receives data from different protocols, including power system specific protocols such as IEC 61850, and general-purpose protocols such as Message Queuing Telemetry Transport (MQTT), and acts as a data broker to send data in the required format to the next simulator. Currently, around 18 different protocols and interfaces are supported. VILLAS node is a C/C++ application optimized for real-time Linux operating systems, and hence can be configured according to the users' needs.

In this work, the VILLAS node is used as an interface between the transmission system simulated in OPAL-RT and the distribution system simulated in the RTDS. The VILLAS node interface with RTDS using the GTNET-SKT card and is responsible for sending or receiving the data. While the VILLAS node interface for RTDS already existed, this work developed the interface between VILLAS node and Hypersim. A new User Coded Module (UCM) is created in the Hypersim folder. This module will be responsible for communicating the data in the Hypersim simulation to the VILLAS node. This module creates a socket connection from the Hypersim computer to the real-time simulator, and then subscribes to the parameters required by the user. These parameters are then communicated via the socket in the form of strings. This implementation is very lightweight and does not occupy much processor space. The Hypersim module developed can be downloaded from the VILLAS node repository [39]. In the co-simulation of these systems, it is essential to consider the effect of latency. The timing diagram in Fig. 2 demonstrates the time taken for data to go through the interface. It is important to perform experiments that can tolerate the latency in communication. By using the VILLAS node, various network tests can be implemented, which allows the user to determine an average latency value. In section III, the issues with latency in federated simulation and its mitigation technique is discussed. The result of the latency experiment is shown in section V.

D. Cyber-Physical Experimentation

The VILLAS node also provides the capability of emulating basic data manipulation such as jitter, packet loss, network latency, and such using Linux's *netem* method. This feature makes it useful to test and perform, geographically distributed co-simulation between different simulators. These features also allow the user to create basic cyber-physical security experiments. Some cases are listed below:

1) Simulating the effect of network latency on control actions by delaying specific measurements,
2) Simulating the effect of missing data points on tools such as state estimation and Phasor Measurement Unit (PMU) based monitoring and control algorithms,
3) Simulating the effect of loss of data quality including noise and jitter on control algorithms, and
4) Simulating a proxy man-in-the-middle attack by delaying and re-ordering the packets.

In addition, the existing testbed capabilities [17] can be used to enable advanced cyber-physical experimentation by using network emulation tools. Tools such as Mininet, CORE, and NS-3 can be used to create Linux containers for the power system node, and this allows us to perform advanced cyber-physical experimentation. Initially, the communication and cyber models need not be federated, as they can be directly connected to the local real-time simulation to create distributed cyber-physical experiments. However, using techniques such as the TAP/TUN on NS-3, it is possible to federate the cyber models too between two testbeds. This aspect of the federation will be explored in the future.

III. Latency Management in Federated Testbed

Communication latency is an essential factor while performing experiments using federated testbed as this may lead to inaccuracies and instability in geographically distributed real-time simulations. The simulators can simulate with the periodicity of milliseconds to microseconds. At the same time, communication latency could be in the order of a few hundred milliseconds or higher for geographically distributed RT simulation. The total latency in the communication network

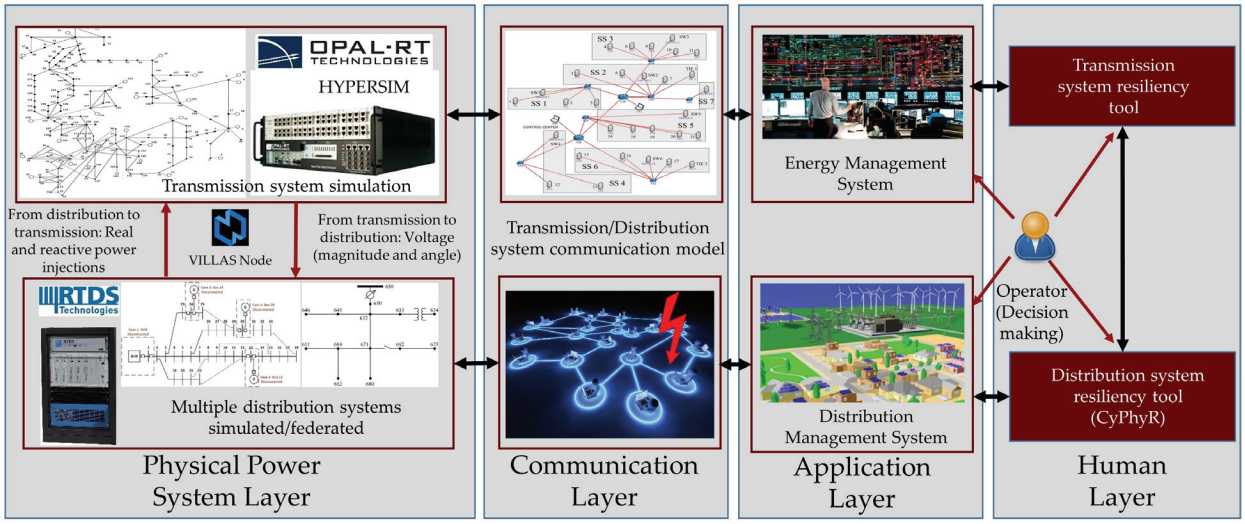

Fig. 1. Cyber-Physical Federated Co-Simulation Testbed

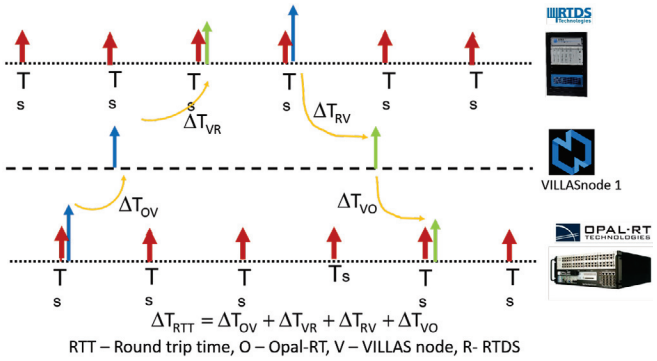

Fig. 2. Timing coordination in co-simulation

can be defined as the addition of four delays, namely, signal propagation delay, network processing delay, transmission delay, and queuing delay [15]. Considering the time span of power system transient events and usual communication delay in the geographically distributed RT simulator, the accuracy and the stability of the simulations will be affected. However, communication latency is unavoidable in geographically distributed real-time simulations. To manage this delay, estimation algorithms can be developed to predict the next set of data with different possible estimation techniques and historical data.

The time frame of the transients defined by Greenwood in [40], typically last from less than a microsecond to several milliseconds. When geographically distributed real-time simulations based on wide area networks are utilized for the analysis of such phenomena, the change in system state can be considered as linear. The idea of linearity for short time-steps of real-time simulation as compared to the Internet latency is also justified by the wide utilization of linear extrapolation in EMTP used by different simulation engines. [41] mathematically demonstrated the utilization of linear extrapolation for EMTP simulation engines. In this work, a linear curve fitting technique is used to address the latency issues as the real-time predictor. The motivation to use the linear regression model for predictions is that during transients event, each peak occurs in approximately 250 ms [15], and the normal range for internet communication latency is a relatively shorter period of time. For this short period, the change in voltage magnitude is small and hence can be considered as linear. Therefore the use of linear interpolation in power system simulation provides a significant improvement in the accuracy of results. Since, linear curve fitting technique is used, predictions are enforced within a time-step of real-time simulation to maintain stability.

Let consider a scenario with two RT simulator used for geographically distributed for real-time data exchange with a data latency of Δt. In another way, Δt is the time for a data packet to travel one-way over the internet. In order to predict accurately, a suitable window size of historical data must be employed as an input. Let N be the number of data points within a window. With the assumption that the changes in received data can be considered as linear within the small period Δt, the target fitting function is defined as in (1)

$$y = ax + b \tag{1}$$

Where a and b are the coefficients of the target linear fit. In order to get the best fitting for N history data points, the target function is formulated as in (2):

$$MinError = \Sigma_{i=1}^{N}(y_i - (ax_i + b))^2 \tag{2}$$

Where y_i is the historical data, and x_i is the related time point.

Figure 3 shows the data flow of the Realtime predictor. At the beginning of the simulation, there is no historical data that can be used to make the prediction, so during the first

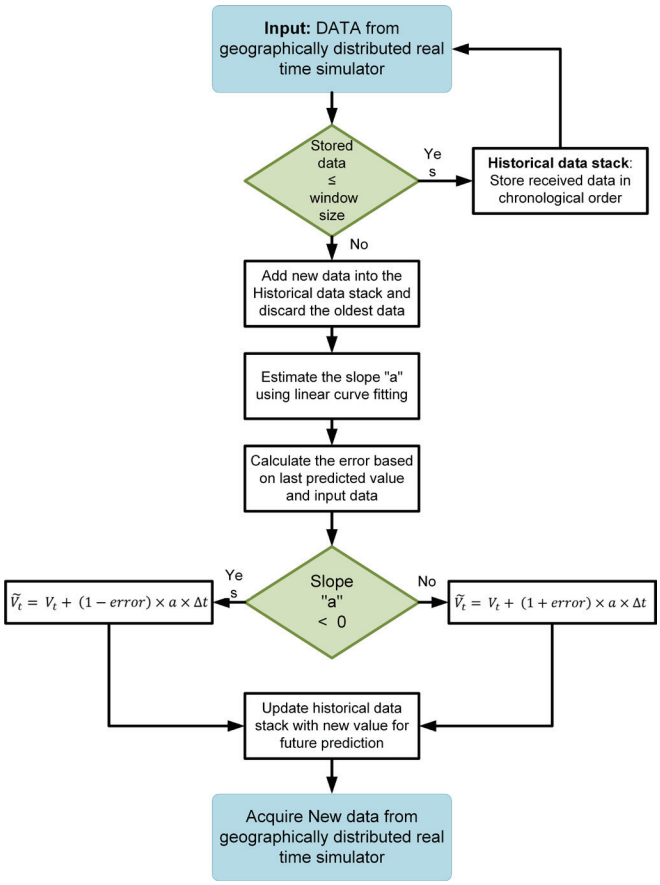

Fig. 3. Realtime linear predictor

N time steps (window size), the input data is stored in a stack. Once the stack is full, slope "a" is computed using the target function in (2). Then, based on the slope "a" and error calculated using (3) to enhance the predictor using the feedback loop, the predicted value V_t at time t is computed.

$$error = \frac{(V_{t+\Delta t} - V_t)}{V_{ref}} \tag{3}$$

Where V_t is the predicted value at time t, $V_{t+\Delta t}$ t is the actual voltage value at time instant t, however, it is received at the remote location at time $t + \Delta t$ due to latency. V_{ref} is the steady state value to normalize the prediction error.

IV. Co-simulation Resiliency Formulation

In general, the effect of changes in transmission system such as line faults, generator failure, or addition of extra generator is studied in terms of other buses in the transmission system analysis. Its effect on specific feeders, or critical loads in the distribution systems are rarely studied. Different changes in the transmission system affect its resiliency in different ways. In this study, the changes in transmission resiliency is demonstrated due to changes in the transmission system and then its effects on the distribution system resiliency.

A. Transmission resiliency formulation

The Cyber-Physical Transmission system Resiliency Assessment Metric (CP-TRAM) [42] is comprised of physical and cyber resiliency scores. The physical resiliency score reflects physical attributes like the physical interconnection of the system, power flows, sources of supply, etc. The cyber score considers all the cyber components under a substation and then aggregated to a system-level score, as explained in the subsections below.

1) Physical Resiliency Score Formulation: The Transmission system physical resiliency score is based on both system infrastructure and operating conditions that enables it to be updated with changing conditions in the system. It is comprised of four components in this study namely:

1) Source-Path-Destination Index (SPDI)
2) MegaWatt Availability Index (MWAI)
3) MegaVAr Availability Index (MVArAI)
4) Supplied Critical Load Index (SCLI)

The SPDI is used to show the effect of topology on the physical network. A graph theory-based approach is used to calculate SPDI. (4) illustrate the mathematical formulation of SPDI.

$$\text{SPDI} = \sum_{i=1}^{N_G} \frac{k_i^2}{\text{BVI}_i \cdot \text{HI}_i \cdot (1 + \text{Average cost}_i)} \tag{4}$$

Where, k_i is the k-number of paths between i^{th} source and destination substation, BVI_i is the Branch Vulnerability Index, HI_i is the Hops Index, Average cost_i is computed in terms of impedance of transmission lines of the network and N_G is the total number of MW sources.

SPDI formulation includes effects of having loops in the meshed network [42]. In Transmission systems, lumped loads connected to transmission substations could be fed from multiple generators. Due to computational burden, the contribution of each path towards the mean electric distance between a generator and feeder substation is considered to choose k-number of paths. This process for a specific feeder substation with critical loads is repeated for all the available generators to handle the meshed network.

The BVI_i index reflects the vulnerability in physical network due to the repetitive occurrence of the transmission lines/transformers in the k-number of paths.

$$\text{BVI}_i = \sum_{N_L} \frac{\frac{n_k}{p}}{k} \tag{5}$$

The BVI_i (5) gives the Branch Vulnerability Index for k-number of paths between MW source i and destination substation, n_k is the number of times a branch occurs in k-number of paths between MW source i and destination substation, p is the number of parallel lines in a multi-circuit transmission line, N_L is the total path and k_i is the k-number of paths between MW source i and destination substation. Hops Index expressed as (6) is computed to reflect the vulnerability due

to number of transmission lines connecting a generator and a substation.

$$\text{HI}_i = \frac{\sum n_{lk}}{k} \tag{6}$$

Where, HI_i is the Hops Index for k-number of paths between MW source i and destination substation,n_{lk} is the number of hops (transmission lines, transformer, etc.) in the k_{th} path between MW source i and destination substation, k_i is the k-number of paths between MW source i and destination substation.

MWAI, MVArAI, and SCLI indices reflect the real-time operating conditions of the physical network and are thus based on real-time measurements.

$$\text{MWAI} = \sum_{i=1}^{N_G} \frac{\text{MWA}_i \cdot \text{GA}_i}{\text{Total MW load}} \tag{7}$$

The MWAI is calculated using (7), MWA is the difference between capacity and generated MW of each source, and *Generator availability* (GA) is introduced into this index based on reliability analysis of generator. For instance, a coal-fired generator has a factor of GA equals to 1.0, whereas, a wind-based generator has a GA of 0.8 due to the uncertain weather conditions.

MVAr availability is calculated as the difference between MVAr capacity of the available reactive power reserves and the actual amount of MVAr used in the system. The ratio of this MVAr availability to total MVAr load gives the MVArAI. Lastly, the SCLI is calculated as the ratio of the critical load supplied to the total critical load present in the system.

After computing all the above-mentioned indices, eq. (8) is used to integrate the individual parameters into a single physical resiliency score (PRS) as in [43] and [44].

$$\text{PRS} = w_1\text{SPDI} + w_2\text{MWAI} + w_3\text{MVArAI} + w_4\text{SCLI} \tag{8}$$

Where the weights are derived using a decision making process called Analytical Hierarchical Process (AHP) [45] with the help of pairwise comparison. Details of this physical resiliency formulation can be found in [46].

2) Cyber Resilience Score Formulation: The transmission resiliency metric CP-TRAM is calculated for each substation. To compute the cyber resiliency score, a detailed substation cyber model is considered, based on the defense-in-depth (DID) model. The defense-in-depth model is a well-known security architecture across various domains, and especially in the industrial control systems (ICS) domain. The DID model secures the system by creating multiple security barriers between the mission-critical physical components and the Internet. DID model is implemented by creating logical layers of separation between various components and Information Technology (IT) and Operations Technology (OT) layers. A representative model of a substation is shown in Fig. 4.

From the DID substation model, an attack graph is generated. The end goal for the attack graph is to compromise the physical power system by sending a malicious trip command to the relay. The attack graph for the DID substation model considered in this work is shown in Fig. 5.

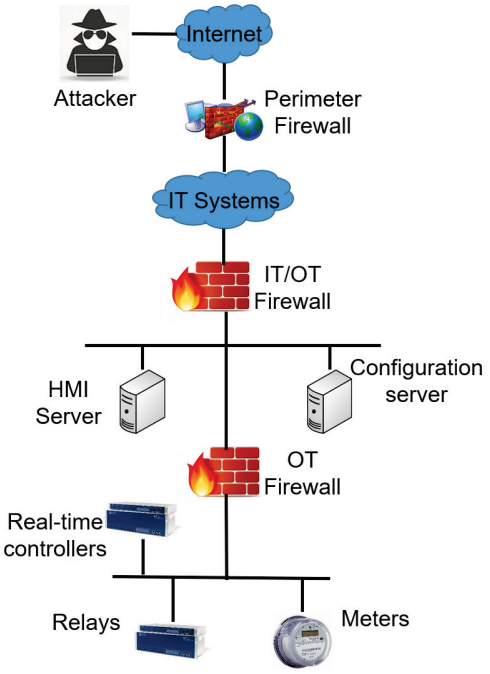

Fig. 4. Defense-in-depth model

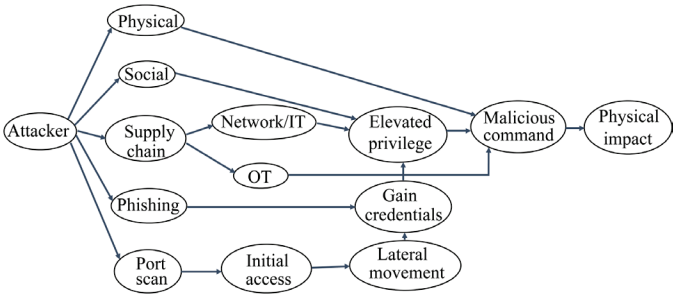

Fig. 5. Attack graph for representative substation model

Based on the attack graph, an Attackability Score (AS) is generated. The AS is considered to be the ratio of the actual number of network paths (N_{NP}) connecting the attacker to the target node to the number of attack paths (N_{AP}), as shown in (9).

$$\text{AS} = \frac{N_{NP}}{N_{AP}} \tag{9}$$

In addition, Impact score has been computed, which is an aggregation of the various security mechanisms present in the model. Various security mechanisms (SM_i) are compared and graded between $(Low, Medium, High)$, and then assigned values $(2, 5, 8)$ based on their grading. These values are used to compute an aggregated security score and can be tuned to particular systems based on the user's requirements. An impact score (IS) has been computed, based on the SCLI at

that particular substation, if there is a physical impact on the power system. The Impact score is defined as,

$$\text{IS} = \frac{\Sigma SM_i}{\text{SCLI}} \tag{10}$$

The AS and IS are combined using a weighted average, where the user can assign the weights. This score is computed for each substation, and then aggregated by the average for all substations, creating a system cyber resiliency score, as defined in (11) where N_S stands for number of substations. This score is then aggregated for all substations, and an average cyber-resiliency score (CRS) is computed for the whole transmission system, to reflect the effect of network-based cyber-attacks better.

$$\text{CRS} = \frac{\Sigma\left[\frac{(w1 \cdot AS_i)(w2 \cdot IS_i)}{(w1+w2)}\right]}{N_S} \tag{11}$$

After obtaining both physical and cyber resiliency score, (12) is used to calculate CP-TRAM.

$$\text{CP-TRAM} = \frac{[w_1 \cdot \text{PRS} \ + w_2 \cdot \text{CRS}]}{(w1 + w2)} \tag{12}$$

Where the weights can be assigned by the user depending on the importance of the physical and cyber aspects of the system. The cyber and physical scores can be integrated using other techniques also, as required by the operator. As the focus of this paper is on the federation of testbed simulation assets for co-simulation, a simplified but complete model is adopted to measure resilience. Interdependence of cyber and physical systems does exist but metrics have been deliberately kept independent to make it easier for root cause analysis to find mitigation and control action to enable resilience as well as meeting the existing operational paradigm.

B. Distribution system resilience

CyPhyR (Cyber-Physical Resilience) tool [44] is used to assess the impact of vulnerabilities on the resiliency. The tool has two stages - (1) planning stage where the vulnerabilities are evaluated in terms of their position in the microgrid, and (2) operational phase where the real-time status of the vulnerability is monitored to determine the impact on the resiliency.

The CyPhyR tool is aimed at improving the microgrid's resiliency. The "big picture" view of the CyPhyR tool is shown in Fig. 6.

In general, contingency management in the power grid is done by planning engineers. So, likewise, the planning engineers will evaluate new vulnerabilities found in the cyber assets during operation. Cyber-assets are defined as cyber-physical devices present in the microgrid, such as controllers, and relays. The planning engineer evaluates these vulnerabilities, provides threat reports, and suggests possible remedial actions in terms of reconfiguration. In the planning phase, a Cyber Asset Impact Potential metric (CAIP) is defined, which calculates the maximum physical impact a particular cyber

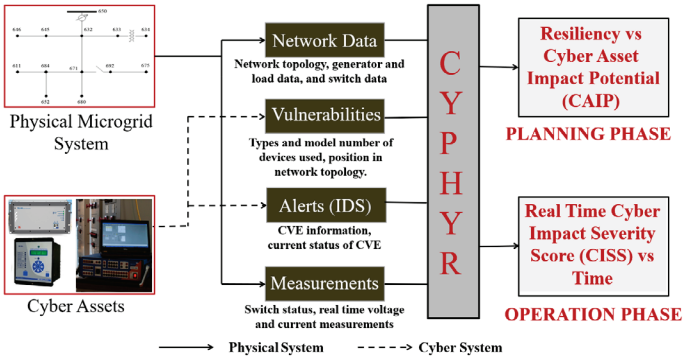

Fig. 6. Cyber-Physical Resilience Impact and Analysis

vulnerability can have on the microgrid, based on the position of the cyber-asset, and the Common Vulnerability Scoring System (CVSS) rating of the vulnerability. In the operation phase, Cyber Impact Severity (CIS) metric is defined, which can determine the resiliency of the microgrid during operation. The CIS metric combines physical measurements from the microgrid, IDS alerts from the communication system, and the CAIP metric. The metric reflects the changing operating conditions of the microgrid and severity of cyber impact. In case of cyber attack or any physical fault, the CIS metric helps the operator to decide on control actions to improve the resiliency of the microgrid, such as isolation of a cyber asset, and reconfiguring the microgrid.

The cyber-physical resiliency is developed across two stages. First, a graph theory-based algorithms considering power system constraints are used to formulate the physical power system resiliency. From the obtained resiliency values and reconfiguration paths, the operation phase cyber-physical resiliency is determined by integrating the real-time measurements and the status of the vulnerabilities in the CIS metric. In this work, the CyPhyR tool is additionally modified to use the CP-TRAM score as the main grid's resiliency during operation. This modification is used to demonstrate the effect of transmission system on the distribution system.

C. Weighting of factors for resiliency metric

The weights to determine the transmission and distribution system resilience are either a weighted sum, or are assigned using a Multi-criteria Decision Making (MCDM) process. This is to provide flexibility to the user to set up the metric as per their requirements. AHP is a technique to solve MCDM problems. Initially, a set of parameters that contribute to the final decision, in this case the resiliency value, are selected. Based on a pairwise comparison method, weights are assigned to each of these factors. The pairwise comparison allows the user to intuitively understand relationships between multiple factors that affect a final decision, in this case the resiliency score. The user can also directly assign weights based on their experience/requirement, but the AHP based pairwise comparison allows us to provide a rigorous method for assigning weights.

V. Results and Discussions

In this section, a federated real-time transmission and distribution co-simulation testbed architecture is demonstrated for validating the proposed approach. In this study, the two RT simulator used for federated testbed architecture are RTDS and OPAL-RT. VILLAS node is used to interface these RT Simulators and manage the co-simulation. It can support both user datagram protocol (UDP) and transmission communication protocol (TCP) for RT communication.

The WECC 179-bus transmission system is modeled in the OPAL-RT (Hypersim). The IEEE 13 Node Test Feeder is used as a distribution system and simulated in the RTDS. In the transmission system, load connected to the bus-106 is simulated as a dynamic load model, which represents the distribution system. Likewise, in the distribution system, the voltage source is connected to node-106 which represents the transmission system. As data exchange, OPAL-RT receives the real and reactive power measurements from RTDS and sends Voltage magnitude and phase angle to OPAL-RT. The federation setup between the OPAL-RT and RTDS is through the VILLAS node, and the interaction between two real-time simulators have been verified in our previous work [17].

A. Resiliency with uncontrolled and controlled islanding

In the first case study, a simple case of islanding is considered. It represents a frequent phenomenon in the power system, with the distribution system being disconnected due to transmission level faults. In some cases, the distribution system might also initiate the disconnection, or the two might be separated due to a cyber-attack. In this case, the systems are assumed to be connected at the beginning of the simulation, and then the systems are disconnected. This results in a sudden loss of load on the transmission system, which changes the transmission system resiliency. In the distribution system, the resilience of the grid changes from the previous transmission system value 1 to 0. This decreases the distribution system resilience because the cheapest and most reliable source of generation is disconnected. The result for this case is shown in Case 1 in Fig 7.

B. Latency Case Study

Since both the simulators are in the same location and are connected via LAN, therefore the interaction latency among them are very minimal. In this setup, the data exchange latency between the two simulators are measured approximately 300 μs. This latency is very less when compared with actual communication latency in geographically distributed RT simulators. Therefore, in this study, a delay of 15 ms is added using time delay block in OPAL-RT to the voltage signal before sending the signal to RTDS via villas node to simulate a typical Internet data latency. The real-time linear predictor is implemented utilizing the user component builder in the RTDS® software to demonstrate the delay mitigation results for data with communication latency. Fig. 8 shows the performance of the latency management using linear predictor by comparing the voltage plot (actual, delayed and predicted

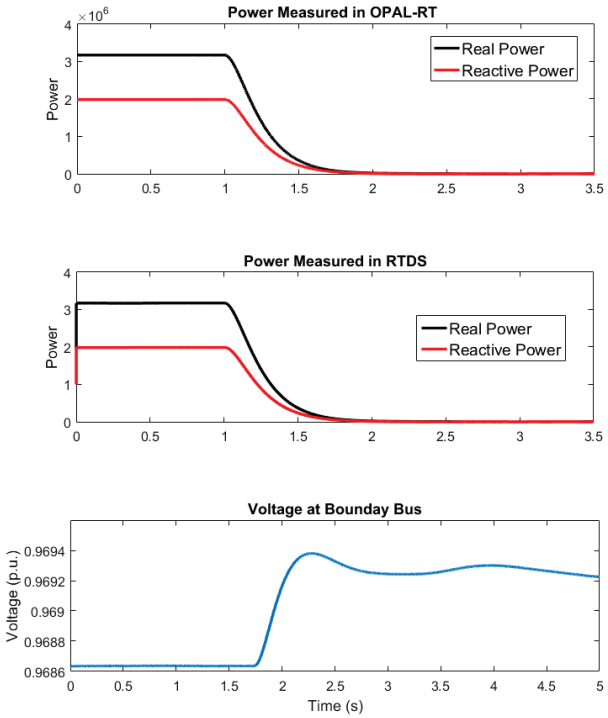

Fig. 7. Islanding of distribution system from transmission.

voltages) for three phase fault scenarios. In this scenario, a fault is created in transmission system. The effectiveness of the real time predictor is assessed using a Unified Evaluation Index (UEI) [15]. The UEI formulation is as shown below:

$$\text{UEI} = \frac{(1 - V_{RMSE} + V_{COR})}{2} \tag{13}$$

Where V_{RMSE} and V_{COR} are the Root Mean Square Errors (RMSE) and the linear correlation coefficient (COR), respectively, UEI is an unbiased weighted average of two factors that are measures of similarity between the actual and delayed/predicted waveforms. This performance metrics set out between 0 to 1. UEI value closer to 1 indicates that the proposed real-time linear predictor output is closer to the real value. Table II show the RMSE, linear correlation coefficient, and UEI of the communication latency case and the prediction case for the three-phase fault scenario. Results show that the real-time linear predictor enhances the accuracy of the co-simulation.

TABLE II
RMSE, COR and UEI for three phase fault

3-phase fault	V_{RMSE}	V_{COR}	UEI
Latency case	0.0080	0.9790	0.9855
Prediction case	0.0025	0.9984	0.9988

C. Transmission system resiliency for various cases

For the transmission resiliency calculation, 4 cases have been considered to demonstrate.

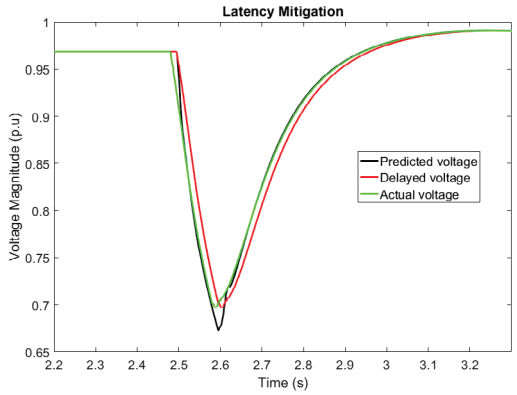

Fig. 8. Latency management using linear prediction.

Case 1: This case is describing the system under normal operating conditions. There is no physical or cyber fault in the system. So, the CP-TRAM of bus 106 of the IEEE 179 bus system is 1, as shown in Table III. The physical resiliency score computed in this case is assumed as the base case, and hence is scaled to be 1. In the case of the cyber-resiliency score, the attackability score is calculated based on (9) as 1/3. The number of attack paths is 3, as the other 2 are not network-based attacks, and the network path is only 1, as the attacker has to compromise the defense depth to gain access. The impact score for this case is 15, as there are three medium rated firewalls (5+5+5) between the attacker and the relay. There is no loss of load in this case, which will also change the Impact score. As with the physical resiliency, assumption are made that these numbers to be the base case, and use them for scaling.

Case 2: Loss of line between bus 104 and 134 is considered here. Physical fault is the reason for this disconnection, and no cyber component is compromised. As a result, the physical resiliency score decreases from the normal operating condition, but the cyber resiliency score remains at 1, and results in a decrease of the CP-TRAM score.

Case 3: For this case, lines between bus 104 - 134, and 101 - 105 are considered lost due to some physical faults. There is no attack or fault in cyber components. Here, physical resiliency decreases more as two lines are out of service compared to one line in case 2. Cyber score also remains unaffected due to the physical phenomenon in the system. The lowering of CP-TRAM value reflects the faults as expected.

Case 4: In this case, a cyber-attack has compromised a generation substation, and created a generator outage at bus 35. The Aurora attack [8] is an example of this type of attack happening on the power grid. From the cyber model shown in Fig. 4, the attacker has compromised the security of the firewalls and gained access to the controller and sent a malicious trip signal to the relay. This results in a significant loss in MW availability, as shown in Table III. In addition, the cyber-resiliency score is also impacted, as the Impact score for that bus goes to 0. Hence, the cyber-resiliency score for the system goes to 0.98, and the CP-TRAM for this case becomes 0.9745.

TABLE III
TRANSMISSION RESILIENCY AT BUS 106

Cases	SCLI	SPDI	MWAI	MVArAI	Physical-resilience score	Cyber-resilience score	CP-TRAM
Case 1	1	40.8192	0.0810	2.6012	1.0000	1	1
Case 2	1	33.2861	0.0807	2.5538	0.9584	1	0.9774
Case 3	1	30.6006	0.0804	2.5490	0.9438	1	0.9719
Case 4	1	40.1608	0.0612	2.2480	0.9690	0.98	0.9745

D. Resiliency of distribution system with loss of generation in transmission

In this case, the effect of transmission system changes on the distribution system resiliency is studied. In practice, the effect of transmission system changes such as generator failure or faults is studied only in terms of other buses. The effect on specific feeders, or critical loads in the distribution systems are rarely studied. In this simulation, the generator at bus 35 is lost, which reduces the resiliency of the transmission system. This also changes the reliability of the transmission system for the distribution system, which is typically assumed to be 100% in practice. The resiliency of the distribution system is then computed, considering the revised transmission system resiliency. As shown in Table III, the transmission system resiliency for this case is computed to be 0.9745. Considering this value of resilience, the distribution system resiliency is then computed as 7.436. The impact of transmission system resilience will be higher or lower, depending on the weight assigned to the CP-TRAM when calculating distribution system resiliency. This is illustrated in Fig. 9, in which the weight assigned to CP-TRAM in distribution system resiliency calculation is varied between 0.15 to 0.35. It is seen that the distribution system resiliency is steadily decreasing as the weight is increasing. The weight can be assigned based on sensitivity analysis, or by user intuition. A more rigorous method will be explored in the future.

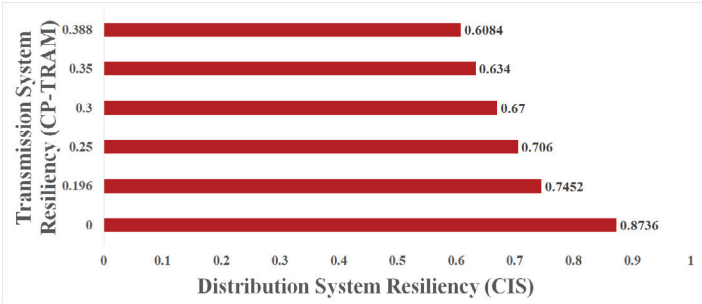

Fig. 9. Effect of CP-TRAM Weights on CIS

VI. CONCLUSIONS

Cyber-transmission-distribution testbeds are required to understand the role of the transmission and distribution operators in making pro-active and corrective decisions to maintain

required system resiliency. Testbed should be able to model the system accurately is needed. In this study, the necessities of testbeds and co-simulation for resiliency analysis and overview of the resiliency assessment tools are demonstrated. Federated co-simulation of the electric transmission and the distribution system and associated cyberinfrastructure is the first step towards this broader effort. In this paper, the requirements for testbed and co-simulation architecture of transmission and distribution detailed model with RTDS and OPAL-RT using VILLASnode are demonstrated. The issue of the communication latency on federated testbed is also presented in this work. The simulation results clearly show that numerical inaccuracy or even incorrect simulation can happen due to large communication latency. To address this issue, a real-time linear prediction method is developed and applied here. Distributed RT federated testbed simulation shows improvement with the implementation of this predictor. A resiliency use-case is studied to demonstrate the importance of co-simulation. Cyber-physical resiliency tools for distribution and transmission systems are presented, and the impact of transmission system resiliency on the distribution system is demonstrated. In the results, the federation of co-simulation is presented, and the effect of latency in real-time operation is examined, and the prediction engine is applied to reduce the simulation error significantly. Resiliency tools based on decision-making methodologies are presented, and scenarios demonstrating the impact of transmission system resiliency on distribution systems are studied for both physical events and cyber-driven events. Future work involves the development of better prediction techniques for highly dynamic scenarios where cyber-physical co-simulation is widely geographically distributed. Furthermore, the application of hardware-in-the-loop (HIL) simulations to leverage geographically dispersed assets as well as federated testbed with cyber-physical-human aspects can be explored.

REFERENCES

[1] E. Shoubaki, M. Arefi, M. Chamana, B. H. Chowdhury, and B. Parkideh, "Time base synchronization for interconnecting real-time platforms in co-simulation," in *2016 IEEE Industry Applications Society Annual Meeting*, Oct 2016, pp. 1–4.

[2] S. Baek, S. Nam, J. Song, J. Lee, T. Kim, and J. Shin, "Design of advanced voltage management system including manual operation mode via real-time digital simulator," *IEEE Transactions on Industry Applications*, vol. 49, no. 4, July 2013.

[3] R. Roofegari nejad, W. Sun, and A. Golshani, "Distributed Restoration for Integrated Transmission and Distribution Systems With DERs," *IEEE Transactions on Power Systems*, vol. 34, no. 6, pp. 4964–4973, 2019.

[4] J. C. Bedoya, J. Xie, Y. Wang, X. Zhang, and C. Liu, "Resiliency of distribution systems incorporating asynchronous information for system restoration," *IEEE Access*, vol. 7, pp. 101 471–101 482, 2019.

[5] Y. Xu, C. Liu, K. P. Schneider, F. K. Tuffner, and D. T. Ton, "Microgrids for service restoration to critical load in a resilient distribution system," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 426–437, 2018.

[6] A. Clark and S. Zonouz, "Cyber-Physical Resilience: Definition and Assessment Metric," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1671–1684, 2019.

[7] J. Taft, "Electric grid resilience and reliability for grid architecture," *Pacific Northwest National Laboratory. https://gridarchitecture. pnnl. gov/media/advanced/Electric_Grid_Resilience_and_Reliability. pdf*, 2017.

[8] M. Zeller, "Myth or reality — does the aurora vulnerability pose a risk to my generator?" in *2011 64th Annual Conference for Protective Relay Engineers*, April 2011.

[9] A. R. Ofoli and M. R. Altimania, "Real-time digital simulator testbed using emegasim® for wind power plants," in *2017 IEEE Industry Applications Society Annual Meeting*, Oct 2017, pp. 1–9.

[10] A. Monti, M. Stevic, S. Vogel, R. W. De Doncker, E. Bompard, A. Estebsari, F. Profumo, R. Hovsapian, M. Mohanpurkar, J. D. Flicker, V. Gevorgian, S. Suryanarayanan, A. K. Srivastava, and A. Benigni, "A Global Real-Time Superlab: Enabling High Penetration of Power Electronics in the Electric Grid," *IEEE Power Electronics Magazine*, vol. 5, no. 3, pp. 35–44, 2018.

[11] K. G. Ravikumar, N. N. Schulz, and A. K. Srivastava, "Distributed simulation of power systems using real-time digital simulator," in *2009 IEEE/PES Power Systems Conference and Exposition*, March 2009, pp. 1–6.

[12] M. O. Faruque, M. Sloderbeck, M. Steurer, and V. Dinavahi, "Thermo-electric co-simulation on geographically distributed real-time simulators," in *2009 IEEE Power Energy Society General Meeting*, July 2009, pp. 1–7.

[13] K. S. Rentachintala, "Multi-rate co-simulation interfaces between the rtds and the opal-rt," Master's thesis, Florida State University, Tallahassee, Florida, 2012.

[14] Q. Huang, J. Wu, J. L. Bastos, and N. N. Schulz, "Distributed simulation applied to shipboard power systems," in *2007 IEEE Electric Ship Technologies Symposium*, May 2007, pp. 498–503.

[15] R. Liu, M. Mohanpurkar, M. Panwar, R. Hovsapian, A. Srivastava, and S. Suryanarayanan, "Geographically distributed real-time digital simulations using linear prediction," *International Journal of Electrical Power & Energy Systems*, vol. 84, pp. 308–317, 2017.

[16] M. Stevic, A. Estebsari, S. Vogel, E. Pons, E. Bompard, M. Masera, and A. Monti, "Multi-site European framework for real-time co-simulation of power systems," *IET Generation, Transmission & Distribution*, vol. 11, no. 17, pp. 4126–4135, nov 2017.

[17] V. Venkataramanan, P. S. Sarker, K. S. Sajan, A. Srivastava, and A. Hahn, "A real-time transmission-distribution testbed for resiliency analysis," in *2019 IEEE Industry Applications Society Annual Meeting*, Sep. 2019, pp. 1–7.

[18] H. Lin, S. S. Veda, S. S. Shukla, L. Mili, and J. Thorp, "Geco: Global event-driven co-simulation framework for interconnected power system and communication network," *IEEE Transactions on Smart Grid*, Sept 2012.

[19] K. M. Hopkinson, K. P. Birman, R. Giovanini, D. V. Coury, X. Wang, and J. S. Thorp, "Epochs: integrated commercial off-the-shelf software for agent-based electric power and communication simulation," in *Simulation Conference, 2003. Proceedings of the 2003 Winter*, Dec 2003.

[20] D. C. Bergman, D. K. Jin, D. M. Nicol, and T. Yardley, "The virtual power system testbed and inter-testbed integration." in *CSET*, 2009.

[21] M. Wei and W. Wang, "Greenbench: A benchmark for observing power grid vulnerability under data-centric threats," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, April 2014.

[22] "A US-Wide DETER-WAMS-ExoGENI Testbed for Wide-Area Monitoring and Control of Power Systems Using Distributed Synchrophasors," http://people.engr.ncsu.edu/achakra2/geni-deter-wams.pdf, accessed: 2016-09-30.

[23] U. Adhikari, T. Morris, and S. Pan, "Wams cyber-physical test bed for power system, cybersecurity study, and data mining," *IEEE Transactions on Smart Grid*, 2016.

[24] G. Dondossola, G. Garrone, J. Szanto, G. Deconinck, T. Loix, and H. Beitollahi, "Ict resilience of power control systems: experimental results from the crutial testbeds," in *2009 IEEE/IFIP International Conference on Dependable Systems Networks*, June 2009.

[25] A. Giani, S. Sastry, K. H. Johansson, and H. Sandberg, "The viking project: An initiative on resilient control of power networks," in *Resilient Control Systems, 2009. ISRCS '09. 2nd International Symposium on*, Aug 2009.

[26] S. Ciraci, J. Daily, J. Fuller, A. Fisher, L. Marinovici, and K. Agarwal, "fncs: A framework for power system and communication networks co-simulation."

[27] B. Palmintier, D. Krishnamurthy, P. Top, S. Smith, J. Daily, and J. Fuller, "Design of the helics high-performance transmission-distribution-communication-market co-simulation framework," in *2017 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, April 2017, pp. 1–6.

[28] M. Blank, S. Lehnhoff, K. Heussen, D. E. Morales Bondy, C. Moyo, and T. Strasser, "Towards a foundation for holistic power system validation and testing," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2016, pp. 1–4.

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

[30] "Measurement challenges and opportunities for developing smart grid testbeds," Available at https://www.nist.gov/system/files/documents/smartgrid/SG-Testbed-Workshop-Report-FINAL-12-8-2014.pdf, December, 2014, summary report by NIST.

[31] "2015 North American grid modernization testbed survey," Available at http://www.sgip.org/wp-content/uploads/2015-North-American-Grid-Modernization-Testbed-Survey.pdf, 2015, Smart Grid Interoperability Panel (SGIP).

[32] R. Liu, C. Vellaithurai, S. Biswas, T. Gamage, and A. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *Smart Grid, IEEE Transactions on*, 2015.

[33] J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *Smart Grid, IEEE Transactions on*, July 2014.

[34] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber physical system security for the electric power grid," *Proceedings of the IEEE*, Jan 2012.

[35] H. Gjermundrod, D. E. Bakken, C. H. Hauser, and A. Bose, "Gridstat: A flexible qos-managed data dissemination framework for the power grid," *IEEE Transactions on Power Delivery*, Jan 2009.

[36] B. T. Richardson and L. Chavez, "National scada test bed consequence modeling tool," *Sandia National Laboratory Report, SAND*, 2008.

[37] R. Kuffel, J. Giesbrecht, T. Maguire, R. Wierckx, and P. McLaren, "RTDS-a fully digital power system simulator operating in real time," in *WESCANEX 95. Communications, Power, and Computing. Conference Proceedings., IEEE*, May 1995.

[38] "Opal-RT Technologies, Montreal, QC, Canada, H3K 1G6," Available at www.opal-rt.com.

[39] "Interfacing VILLASnode and Hypersim," https://villas.fein-aachen.org/doc/node-client-hypersim.html/, accessed: 2019-02-01.

[40] A. Greenwood, "Electrical transients in power systems, 2nd edition," 1 1991.

[41] J. R. Marti and J. Lin, "Suppression of numerical oscillations in the emtp power systems," *IEEE Transactions on Power Systems*, vol. 4, no. 2, pp. 739–747, 1989.

[42] Tushar, V. Venkataramanan, A. Srivastava, and A. Hahn, "CP-TRAM: Cyber-Physical Transmission Resiliency Assessment Metric," *IEEE Transactions on Smart Grid*, pp. 1–1, 2020.

[43] V. Venkataramanan, A. Hahn, and A. Srivastava, "CP-SAM: Cyber-Physical Security Assessment Metric for Monitoring Microgrid Resiliency," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 1055–1065, 2020.

[44] V. Venkataramanan and A. Hahn and A. Srivastava, "CyPhyR: a cyber-physical analysis tool for measuring and enabling resiliency in microgrids," *IET Cyber-Physical Systems: Theory Applications*, vol. 4, no. 4, pp. 313–321, 2019.

[45] B. L. Golden, E. A. Wasil, and P. T. Harker, *Analytic hierarchy process*. Springer, 2003, vol. 113.

[46] Tushar, "Measuring and Enabling Cyber-Physical Resiliency of Electric Transmission Systems," Ph.D. dissertation, Washington State University, Pullman, WA, 2018.