# CP-TRAM: Cyber-Physical Transmission Resiliency Assessment Metric

Tushar, *Member, IEEE*, V. Venkataramanan, *Member, IEEE*,
A. Srivastava, *Senior Member, IEEE*, and A. Hahn, *Member, IEEE*

***Abstract*—Natural disasters and cyber intrusions threaten the normal operation of the critical electric grid infrastructure. There is still no widely accepted methodology to quantify the resilience in power systems. In this work, power system resiliency refers to the ability of the system to keep provide energy to the critical load even with adverse events. A significant amount of work has been done to quantify the resilience for distribution systems. Even though critical loads are located in distribution system, transmission system play a critical role in supplying energy to distribution feeder in addition to the Distributed Energy Resources (DERs). This work focuses on developing a framework to quantify the resiliency of cyber-physical transmission systems. Quantifying the resiliency of the transmission network, is important to determine and devise suitable control mechanisms to minimize the effects of undesirable events in the power grid. The proposed metric is based on both system infrastructure and with changing operating conditions. A graphical analysis along with measure of critical parameters of the network is performed to quantify the redundancy and vulnerabilities in the physical network of the system. A similar approach is used to quantify the cyber-resiliency. The results indicate the capability of the proposed framework to quantify cyber-physical resilience of the transmission systems.**

***Index Terms*—Transmission resiliency, cyber resiliency, cyber-physical resiliency.**

## I. Introduction

LARGE scale power outages caused by natural disasters (e.g., floods and hurricanes) and cyber-attacks (e.g., Ukraine attack) have highlighted the importance and urgency to improve grid resilience of the US. According to [1], the number of outages caused by severe weather is expected to rise as climate change increases the frequency and intensity of hurricanes, blizzards, floods and other extreme weather events. Thus, in anticipation of such extreme events in future, it is essential to build more resilient critical infrastructures [2]–[5].

Resiliency studies focus on the ability of the system to withstand extreme events and focus on supplying critical/priority loads. Change in resiliency metric of the system can be used to make decision for investing limited resources wisely in enhancing resilience. Metrics are being developed for both the transmission and distribution systems. Several researchers have focused on studying resiliency of the power system from distribution system's point of view like [6]–[16]. Disruptions in distribution systems are more local as compared to disruptions in transmission systems, which is a wide-area problem impacting resilience of multiple distribution feeders. Thus, it is very important to study the resiliency of transmission systems. Authors in [17] and [18] focus on transmission resiliency calculation based on a probabilistic approach under severe weather-based adversaries. This paper aims to provide a framework for quantifying the concept of cyber-physical resiliency especially in transmission systems.

Recent power outages caused by cyber events such as Ukraine Attack, have highlighted the importance and urgency to improve grid resilience [19], [20]. Supervisory Control And Data Acquisition (SCADA) are vulnerable to external remote cyber threats as discussed in [21]. Cyber vulnerabilities that exist in the SCADA and Energy Management Systems (EMS) have been discussed in [22]–[24]. Certain methods to assess vulnerabilities in the cyber network of power system have been discussed in [25]–[27]. According to 2015 Dell Security Annual Threat Report, the world-wide SCADA attacks increased from 91,676 in January, 2012 to 675, 186 in January, 2014. This risk was exemplified on December 23rd, 2015 in Ukraine [28]. Cyber vulnerability in SCADA devices at the substations is being recognized as one of the critical issues [29] as any planned attack on substations may lead to cascading outages in the power systems [30]. Cyber attackers could spend a long term to conduct illegal reconnaissance activities such as port scanning and spear phishing, and to exploit existing vulnerabilities. After gaining critical information and controllability of the target substation, attacker can launch disruptive cyber attacks easily. For an example, the Stuxnet malware was used to compromise power facilities after years of reconnaissance activities [31], [32].

Intelligent electronic devices (IEDs) and in general, measurement devices with embedded communication and data processing, are used for different levels of control and protection in power systems. IEDs and associated cyber systems are subject to above vulnerabilities. Cyber-physical resiliency metric will help in decision making to patch some of the

Manuscript received July 30, 2019; revised March 14, 2020; accepted May 13, 2020. Date of publication May 20, 2020; date of current version October 21, 2020. This work was supported in part by the Department of Energy under Award DE-OE0000780, and in part by NSF FW-HTF under Award 1840192. Paper no. TSG-01105-2019. *(Corresponding author: A. Srivastava.)*

Tushar was with the School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99163 USA. He is now with the GE Digital, Redmond, WA 98052 USA.

V. Venkataramanan was with the School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99163 USA. He is now with the Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139 USA.

A. Srivastava and A. Hahn are with the School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99163 USA (e-mail: anurag.k.srivastava@wsu.edu).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2020.2996137

vulnerabilities or isolate some of the cyber assets in operation as needed driven by metric.

We believe our work is one of the first to define 'system characteristic based cyber-physical resilience' for transmission system instead of limited existing work on performance-based metrics. The main contributions of this paper are as follows:

- Factors affecting cyber-physical resiliency of transmission systems are outlined and computed.
- A framework for quantifying the effect of physical infrastructure on resiliency is proposed.
- A framework for quantifying the effect of cyber infrastructure on resiliency is proposed.
- A framework for integrating factors for quantifying the cyber and physical resiliency.
- Validation of the developed resiliency framework through case studies.

The resiliency metric framework proposed in this work does not consider power system dynamics and transient behavior during switching actions following our definition. The protection system in the network is assumed to be capable of changing network topology, loops, and reverse power flows. The resiliency metric is calculated after the protection system actions and is useful for providing situational awareness to the operator and assist in performing corrective control action after an event.

## II. Physical Resiliency Metric

The term *resilience* has been used in various disciplines in their own respective applicable systems like ecological systems, social systems, organizational systems. Each discipline has its own way of defining resiliency, ecological systems [33], economic systems [34], social systems [35]. All these definitions have a similar concept for resiliency but with domain-specific differences.

The challenges in quantifying resiliency for transmission systems unlike distribution systems are:

- Transmission networks are usually meshed networks as compared to distribution networks which are mostly radial in nature.
- Transmission networks have multiple sources of power supply that need to be taken into account while estimating the performance of the system.
- Meshed topology creates redundancy in the network paths and hence needs to be taken into account.
- All transmission-level substations can have critical/priority loads. Thus, a single metric cannot asses resiliency of all critical/priority loads in a transmission network.

*Definition:* Cyber-physical resilience is the ability to avoid or withstand grid stress events without suffering operational compromise or to adapt to and compensate for the resultant strains so as to minimize compromise via graceful degradation.

Our definition of cyber-physical resilience for transmission grids is adapted from the recent Department of Energy (DoE) publication on the definition of resilience [36]. Our proposed resilience metric thus aims to quantify the ability of the transmission grid to supply power to its critical loads at all substations, in the face of grid stress events.

The physical resiliency metric is quantified based on a mix of *infrastructure* and *operational* indices. The various attributes that are used to define the physical resiliency of the transmission system include:

- Network configuration of the system
- Redundancy in the system (both network and source)
- Vulnerability due to repeated use of a particular resource
- Physical stability of the system
- Variability and availability of the power supply

The developed physical resiliency metric comprises of four components:

1) Source-Path-Destination (SPD) index
2) MW availability index
3) MVAr availability index
4) Loss of Load index

It is important to note here that these carefully selected factors are included in the calculation of resiliency for power grid network based characteristics to impact resiliency such as: line outages, bus outages, generator and load outages, loss of multi-circuit lines, network reconfiguration, etc. As the proposed physical resiliency index will be a integration of different possible factors (as explained later in this section), additional factors can be added to suit specific systems under study.

### A. Source-Path-Destination Index

The power grid is a complex network structure that naturally lends itself to be analyzed as a graph. Power grids have been analyzed as complex network graphs in literature [37]–[40], and a number of topological metrics that affect performance have been proposed [37], [41], [42]. For our definition of resilience, the topology of the power grid is important to ensure that the critical loads at all substations are supplied with multiple possible paths. Considering that resilience becomes important in stressed grid conditions, a topology-based metric is important to analyze the changing nature of the topology, and its effect on resilience. The SPD index is a topological-structure-based index that includes various factors like multiple transmission paths from source to feeder, redundancy in generation sources, multi-circuit transmission lines, vulnerability in transmission lines due to repetitive occurrence in all transmission paths. The SPD index is mathematically computed using the below formula:

$$\text{SPD index} = \sum_{i=1}^{N_G} \frac{k_i^2}{\text{BVI}_i * \text{HI}_i * \left(1 + \text{Average cost}_i\right)} \tag{1}$$

where,

'$k_i$' is the k-number of paths from a MW source 'i' to destination substation

'$\text{BVI}_i$' is the Branch Vulnerability Index

'$\text{HI}_i$' is the Hops Index

'Average $\text{cost}_i$' is computed in terms of electrical distance of the network

'$\text{N}_G$' is the total number of MW sources

The formulation in Eqn. (1) is an empirical formulation driven towards measuring the effect of topology changes on the ability of the grid to supply critical loads. In particular,

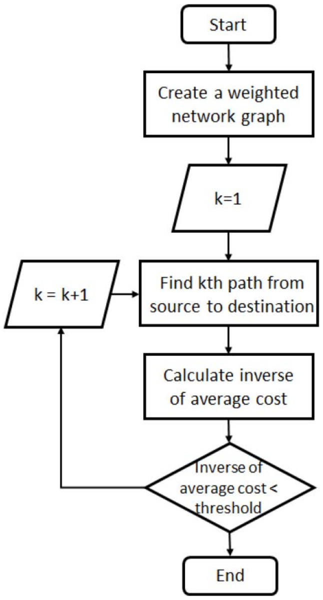
Start
Create a weighted network graph
k=1
k = k+1
Find kth path from source to destination
Calculate inverse of average cost
Inverse of average cost < threshold
End

Fig. 1. Flow chart for computation of k-shortest paths.

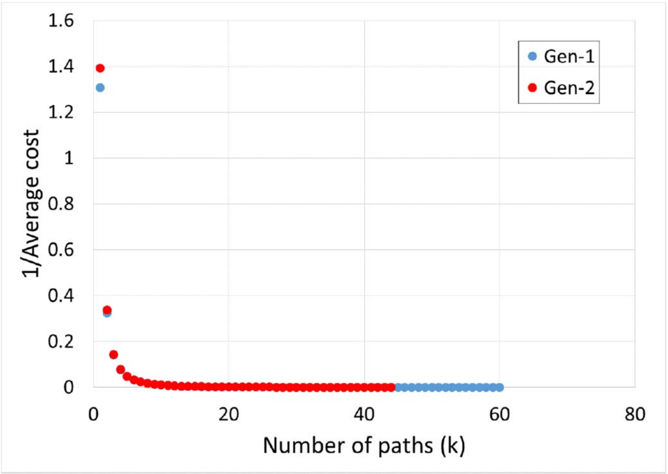

Fig. 2. k-number of paths for bus 12.

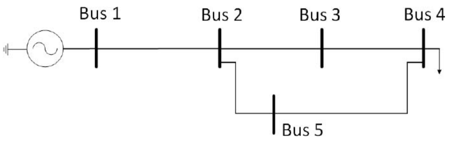

Fig. 3. 5 bus test system.

TABLE I
COMPUTATION OF BVI FOR 5 BUS TEST SYSTEM

| S.No. | Lines | | 'k' | $\frac{n_k}{k}$ |
|---|---|---|---|---|
| | From Bus | To Bus | | |
| 1 | 1 | 2 | 2 | 1.0 |
| 2 | 2 | 3 | 2 | 0.5 |
| 3 | 4 | 5 | 2 | 0.5 |
| 4 | 3 | 4 | 2 | 0.5 |
| 5 | 2 | 5 | 2 | 0.5 |
| | **BVI** | | | 3.0 |

when considering the power grid as a graph, the SPD index is an extension of the edge connectivity of the graph. The edge connectivity represents the maximum number of edges that can be removed while still having a complete graph and a way to measure redundancy in number of possible paths to supply critical loads. The effect of the individual topology metrics on the connectivity is straightforward [37], [42], and the SPD index provides a framework to combine them for studying resiliency during extreme events.

*1) Calculation of K-Number of Paths From a Source to Destination:* Transmission systems have multiple generators connected in the system. All these generators could be used to supply a lumped load connected at the end of transmission substations. It becomes computationally very expensive to compute all paths between all generators and a load substation. Thus, only k-number of paths are chosen based on the contribution of each path towards mean electric distance between a generator and feeder substation. The assessment is based on the k-shortest paths algorithm [43]. This algorithm is used to calculate $k$ number of paths between a MW generation source and a destination substation. The number $k$ is based on the number of paths that contribute to the average cost between a MW generation source and destination load substation. In this paper, impedance of transmission lines is used as the cost factor. After a certain $k$ number of paths, the inverse of average impedance becomes constant. The algorithm to compute the $k$ paths is shown in Fig. 1.

For instance, in case of IEEE 14 bus [44] system, (Fig. 2), it is observed that there are a total of 60 paths from generator at bus 1 to load substation at bus 12. The k-number of paths that contribute to the average cost of these paths is 18.

*2) Calculation of BVI:* Branch Vulnerability Index is computed to reflect the vulnerability in the physical network due to repetitive occurrence of the transmission lines/transformers in the k-number of paths, i.e., if a particular transmission lines occurs in all k-number of paths between a generator and a feeder substation, then that particular transmission line has a higher impact on resiliency as compared to other transmission lines. This index also takes into account the effect of multi-circuit transmission lines in the system.

$$\mathrm{BVI}_i = \sum_{N_L} \frac{(n_k/p)}{k} \tag{2}$$

where,

'$\mathrm{BVI}_i$' is 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

'$k_i$' is the k-number of paths between MW source $i$ and destination substation

Fig. 3 shows a test system to illustrate the various metrics used in the calculation of physical resiliency.

Table I shows the BVI computed for the 5 bus test system. It can be observed here that $k = 2$ as there are only two alternate paths from MW source to destination load. The value of '$p$' is 1 here as there are no multi-circuit lines in the test system. The

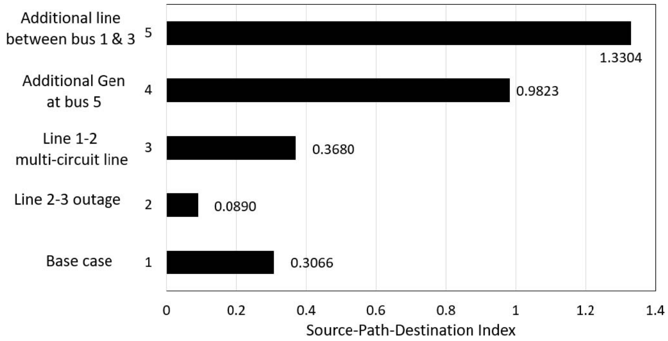

Fig. 4. SPD index for various cases in the 5 bus test system.

line $1-2$ occurs in both these alternative paths and hence has a greater contribution to the BVI of the system as compared to other lines.

*3) Calculation of HI:* Hops Index is computed to reflect the vulnerability due to number of transmission lines connecting a generator and a substation and calculated as follows:

$$\mathrm{HI}_i = \frac{\sum n_{lk}}{k} \tag{3}$$

where,

'$\mathrm{HI}_i$' 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) in the kth path between MW source $i$ and destination

'$k_i$' is the k-number of paths between MW source $i$ and destination substation

For instance, the Hops Index for 5 bus system, (Fig. 3) is:

$$\mathrm{HI} = \frac{3+3}{2} = 3$$

Once, all the individual metrices (k paths, BVI, HI) are calculated, these can be combined together to form the SPD index. Fig. 4 shows the SPD index calculated for different operating cases in the 5 bus system.

### B. MW Availability Index

This index is based on the physical availability of MW sources for critical loads in the system. For example, a coal or hydro-based generator has a higher availability factor as compared to solar or wind based generator due to natural variations. The availability factor may also include factors like ramp rate of generators. The MW availability index is calculated as:

$$\text{MW availability index} = \sum_{i=1}^{N_G} \frac{\text{MW availability}_i * \text{Availability Factor}_i}{\text{Total MW load}} \tag{4}$$

where, '$N_G$' is the total number of MW sources

The 'MW availability' is calculated as the difference between MW capacity and the actual MW used in the system based on the measurements from the SCADA/PMU.

The 'Generator availability (GA)' could be computed based on reliability analysis of generator [45].

### C. MVAr Availability Index

This index is based on the ability of the system to control voltage at a substation so that an acceptable voltage profile is maintained. Only those sources of reactive power are considered for a particular load bus that are included in its voltage control area. The voltage control area is computed based on electric distance (based on Jacobian matrix) and hierarchical classification algorithm [46]. The MVAr availability index is computed as:

$$\text{MVAr availability index} = \sum_{N_{RR}} \frac{\text{MVAr availability}}{\text{Total MVAr load}} \tag{5}$$

where,

N$_{RR}$ is the total number of reactive reserves available in the voltage control area of the substation.

'MVAr availability' is calculated as the difference between MVAr capacity of the available reactive power reserves and the actual amount of MVAr used based on the measurements from the SCADA/PMU.

### D. Loss of Load Index

This index is computed to factor-in the amount of critical loads being supplied as compared to the total critical load at each substation. The loss of load index is computed as follows:

$$\text{Loss of load index(LoLI)} = \frac{\text{Actual Critical load supplied}}{\text{Total critical load}}. \tag{6}$$

### E. Formulation of Physical Resiliency Metric: AHP Formulation

Four factors that contribute to the physical resiliency score have been described. These parameters can be considered as a tuple that describes that physical resiliency. However, operators in control centers might prefer a single intuitive score that can be used to quickly understand the state of the system. Hence, these metrics are integrated using a Multi Criteria Decision Making (MCDM) problem framework which allows the operator to weight individual parameters according to their requirements or automatically following AHP. Analytical Hierarchical Process (AHP) method [47], can be used to solve this problem and user can evaluate the importance of each criterion. The scale of importance can be based upon discussion with experts based on the fundamental scale as shown in Table II. Although the final resiliency score is reported as a single number, it will be easy to understand the contributions of individual parameters to the resiliency once the weights are calculated. The flexibility to assign weights also allows easy implementation of the metric for different systems. Additionally, all the factors are directly accessible, if needed and for root cause analysis. Another important point to note here is that CP-TRAM is computed for each bus separately, so effect of geographical distance or changing environment will not be a factor.

The AHP generates a weight for each evaluation criterion according to the decision maker's pairwise comparisons of the attributes [47]. All the above mentioned computed indices are

TABLE II
FUNDAMENTAL SCALE USED FOR PAIRWISE MATRIX IN AHP

| Intensity of Importance ($a_{jk}$) | Definition |
|---|---|
| 1 | $j$ and $k$ are equally important |
| 3 | $j$ is slightly more important than $k$ |
| 5 | $j$ is more important than $k$ |
| 7 | $j$ is strongly more important than $k$ |
| 9 | $j$ is absolutely more important than $k$ |

integrated using AHP to compute a single physical resiliency metric at each transmission-level substation.

## III. CYBER RESILIENCY FOR TRANSMISSION SYSTEM

There is a need to develop a cyber resiliency metric along with physical resiliency metric to provide quantitative insights into ability of communication and cyber system to ensure operational resilience. The topology of the power system and the communication system are assumed to have isomorphic graph structure. This means that the structure of the network topology for the two systems remains broadly same in this study and can be changed based on the real system configuration. This assumption can be supported by industrial practices where for the high voltage networks the communication topology is typically point-to-point fiber based Synchronous Digital Hierarchy (SDH) networks [48], [49]. Considering the isomorphic nature of the topology, we derive parallels between the factors affecting the physical resiliency and communication resiliency. Hence, our cyber resiliency score is a measure of the ability of the cyber system to support the physical power grid to supply its critical loads in face of grid stress.

It has been commonly observed that the organizations are reluctant to change their security policy or patch their machines even in the face of evidence that their network is vulnerable to attack. For example, an organization may choose to keep an FTP server open, or give its employees remote access to files and ability to work from home.

The Common Weakness Enumeration (CWE) [50] framework classifies software security weaknesses, and has arranged the weaknesses into lists based on their types. With the increase in attack surface, various defensive tools are emerging, such as improvised fire-walls, intrusion detection system (IDS), anomaly detection system (ADS), etc. Such defensive tools try to stop malicious activities by monitoring and analyzing the transmitted data packets.

The physical resiliency score is computed for individual buses at the transmission level. Similarly, to compute the cyber resiliency score, we consider a detailed substation cyber model, based on the defense-in-depth (DID) model. The defense-in-depth model is a well known security architecture [51] 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 public network. 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. 5.

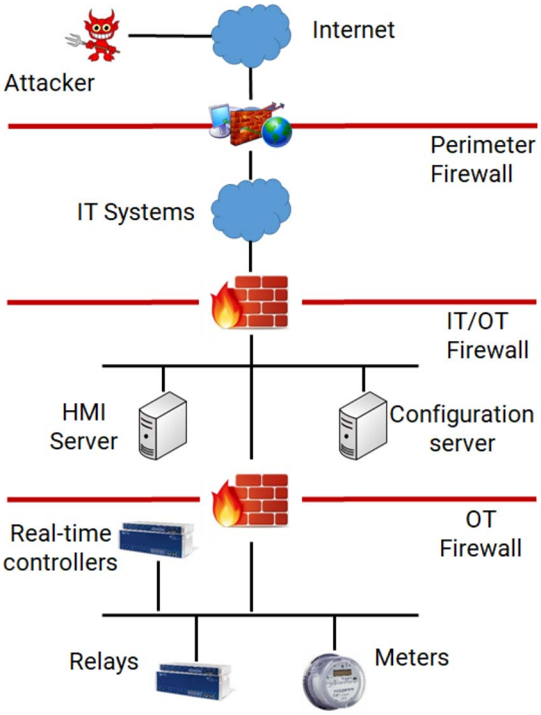

Fig. 5. Defense-in-depth model.

TABLE III
COMPARISON OF PHYSICAL & CYBER RESILIENCY METRIC

| Factors affecting Physical resiliency | Factors affecting Cyber resiliency |
|---|---|
| Network configuration of the power system network | Network configuration of the communication network |
| Redundancy in paths/sources | Redundancy in communication network(e.g., star topology, point-to-point topology) |
| Number of hops (transmission lines, transformers, etc.) | Number of security mechanisms |
| Vulnerability in transmission lines due to its repetitive occurrence in k-paths | Possible attack paths to an attacker (point of access to end devices) |
| MW availability in the system | Available bandwidth in the communication network |
| MVAr availability in the system | Latency in the communication network |
| Loss of critical loads | State of the device (whether it is compromised or not) |

Measuring the resiliency level of the cyber system in the substation can aid system engineers to revisit the network design for achieving satisfactory levels of security. The proposed cyber resiliency metric for transmission systems is analyzed analogous to the physical resiliency metric for the network part, as the graph structure of the two systems are isomorphic. Also, the objective of the physical and cyber metric are both to measure the ability of the grid to supply its critical load, and hence similar factors affect both systems. The comparison between the physical and cyber systems are described in Table III.

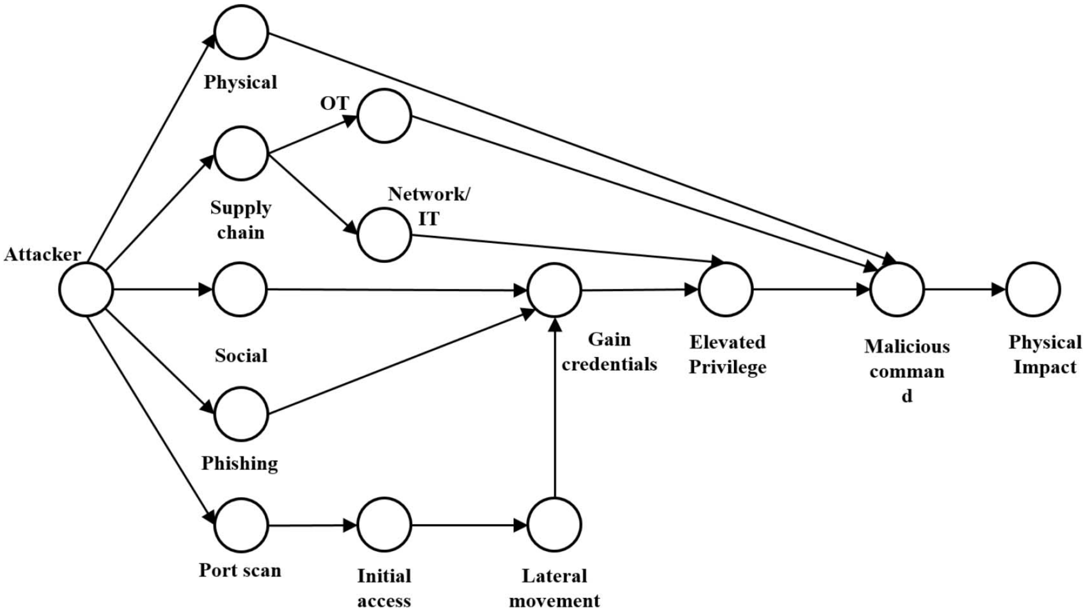

Fig. 6. Attack graph for representative substation model.

Some of the factors that affect the cyber resiliency metric include:

- Quality of Service (QoS)
- Vulnerabilities in the communication network
- Security mechanisms deployed in the network.

### A. Quality of Service (QoS)

Quality of Service (QoS) is essential to ensure that the control commands reach the desired end node in a timely and accurate manner. Hence we consider that QoS metrics such as latency, jitter, and packet drop in our cyber resiliency score. The traditional QoS in system communications is based on the latency and data rate [52]. Thus, the parameters measuring QoS depend on the topology of the communication architecture used in the system. For example, the different types of Ethernet switch based architecture include: cascaded, ring, and star or combination of either of them. Table IV lists a comparison of various architectural implementation and their implications of latency, redundancy, etc. It can be observed that a basic star architecture may provide the least latency in the communication network but may result in very low redundancy, i.e., if a communication link between an IED and router switch is lost then it would result in complete loss of communication. On the other hand, if a redundant ring structure is implemented (that provides high redundancy), it results in higher cost and latency. Thus, a balanced architecture is selected based on the timing requirements of the application.

Along with latency and bandwidth, the QoS requirements also consider Confidentiality, Integrity and Authentication of the communication messages. The messages such as trip commands, interlocking, are sent via GOOSE messages in a substation. Thus, these messages are time critical and need to be highly reliable. Thus, it is a challenge to meet both the security and timing requirements as the use of security mechanisms adds overhead time.

TABLE IV
COMPARISON OF DIFFERENT ARCHITECTURAL IMPLEMENTATION OF ETHERNET-BASED COMMUNICATION NETWORK

| Configuration | Implementation | Cost | Latency | Redundancy |
|---|---|---|---|---|
| Cascaded | simple | low | high | none |
| Ring | complex | medium | high | low |
| Star | simple | medium | low | none |
| Star-Ring | complex | high | low | medium |
| Redundant ring | complex | high | medium | high |

### B. Vulnerabilities in the Communication Network

There may be several vulnerabilities in the existing communication infrastructure deployed in a smart substation. One of the ways to explore the consequence of these vulnerabilities is to form an attack graph. An attack graph is a representation of the paths an attacker can take to exploit vulnerabilities in the network. This give an insight to the various attack paths available to the attacker, i.e., point of access to end devices.

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 our DID substation model is shown in Fig. 6. Based on the attack graph, an attackability score is generated. The attackability score is considered to be the ratio of the actual network paths connecting the attacker to the target node to the attack paths, as shown in Eqn. (7).

$$\text{Attackability} = \frac{\text{Number of network paths}}{\text{Number of attack paths}}. \tag{7}$$

### C. Security Mechanisms Deployed in the Network

In this section, we assess the security measures deployed in the cyber infrastructure of the substation quantitatively to include in the cyber resiliency metric. A security graph based technique is used to quantify the effect of security mechanisms deployed in the system. The security graph is similar to an attack graph wherein the vulnerabilities are replaced with security mechanisms. In the security graph, the paths between two communication nodes (e.g., between a RTU and a station bus router) are weighed based on the security mechanisms being used in between these two communication nodes. The weight of the path reflects how secure the communication paths is between the nodes as compared to other communication paths. The weights are assigned based on a multi-level AHP.

The security mechanisms deployed in the substation may be broadly classified into the following categories:

1) Authentication mechanisms
2) Monitoring and logging security mechanisms
3) Access control mechanisms
4) Encryption of data using cryptography techniques
5) Attacker capability and knowledge
6) Employee preparedness and training

Table V shows the security mechanisms considered, and a simple *(Low, Medium, High)* distinction that can be used to assign weights to the security mechanisms.

In the first level of AHP, the categories are listed in the pair-wise comparison matrix and weights are found based on the user's choice and preference. Once the weights for the security categories are found, security mechanisms in each security category is then listed in the pair-wise comparison matrix of the AHP in the next level. In this way, a multi-level weightage is found to the security mechanisms deployed in the network. A detailed discussion on how the weights assigned in described in the following section. The path with lowest security mechanisms from the attacker's point of access to the control IEDs (as an example of attacker's target) is found and is considered to be characteristic path for that device w.r.t security point of view. The security scores of each control IED at a substation are then combined to obtain a single score for a substation known as attack-ability score using the following equation:

The Security score is then defined as,

$$\text{Security score} = \frac{\Sigma(SM_i * AHP\ Weight)}{\text{Impact value}} \tag{8}$$

where,

Impact value is calculated based on the amount of utilization of the transmission lines if that particular IED is taken out of service. The impact value is given as:

$$\text{Impact value} = \sum_{\text{lines}} \frac{\text{P}}{\text{P}_{\text{max}}} \tag{9}$$

where,

P is the amount of power flowing in each line after the IED is taken out

$\text{P}_{\text{max}}$ is the maximum rating of that line

The Attackability and Security score are combined as a weighted sum, where the weights can be assigned by the user as defined in Eqn. (10). This score is computed for each individual substation, and then can be aggregated as an average for all substations, creating a system cyber resiliency score.

$$\text{Cyber resiliency} = \left(w_1 * \text{Attackability}_i\right) + \left(w_2 * \text{Security}_i\right) \tag{10}$$

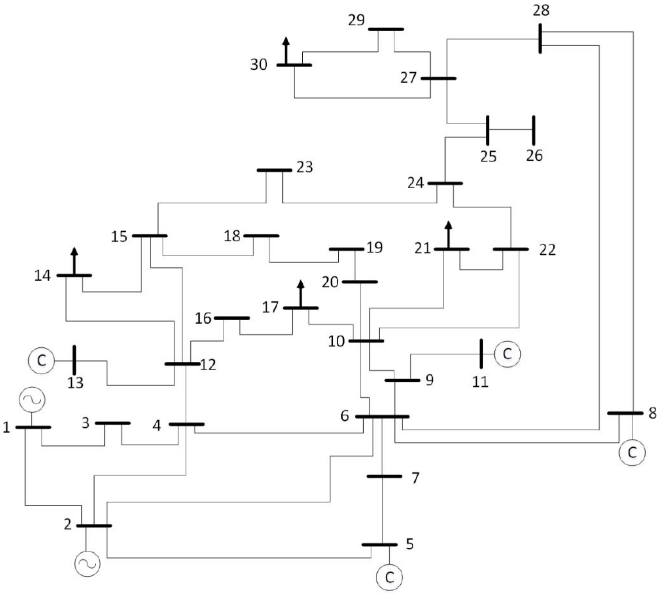

Fig. 7. 30 bus test system.

An important consideration for cyber resiliency is the concept of "safe partition" or "airgap" between the IT and OT networks. While many power grid assets are separated from the Internet, some assets are discovered online, as evidenced by resources such as Shodan. Safe partition can be modeled through cyber graph network and considered in cyber resiliency metric. In addition, the following concerns exist -

1) Airgapping might not be foolproof as some utilities might not follow the recommended practice
2) Vulnerabilities exist (and are being discovered) that allow for bridging between networks
3) Even in best case scenario, airgap does not prevent insider/hardware (such as USB)/supply chain based attacks

Hence it is important for utilities to keep track of their cyber-resiliency even if they are practicing partitioning methods.

## IV. Results

### A. Case Study for Physical Resiliency

To demonstrate the proposed physical resiliency metric, the methodology is implemented on IEEE 30 bus system [44] as shown in Fig. 7.

Once, all the inputs are obtained, all the individual indices can be calculated and combined to form a single physical resiliency metric at each substation. Various events were simulated and the physical resiliency was estimated for each case as shown in Fig. 8. For the ease of explanation, it is assumed that critical/priority loads are located at buses 14, 17, 21, and 30. It can be observed that for events that deteriorate the performance of the system the physical resiliency metric also

TABLE V
LEVELS OF SECURITY MECHANISMS DEPLOYED IN SUBSTATIONS

| **Security Mechanism** | **Description** | **Low** | **Medium** | **High** |
|---|---|---|---|---|
| SM1 | Authentication | No authentication | Role based | Multi-factor |
| SM2 | Monitoring | No monitoring | Intrusion Detection System (IDS) | Security Information and Event Managment (SIEM) |
| SM3 | Access control | General firewall | Intrusion Protection System (IPS) | Firewall + Virtual Private Network (VPN) |
| SM4 | Data integrity | No encryption | Low level (asymmetric key encryption) | High level (symmetric key encryption) |
| SM5 | Attacker capability | Low | Medium | High |
| SM6 | Employee Preparedness | No training | Educational programs | Planned penetration testing and training |

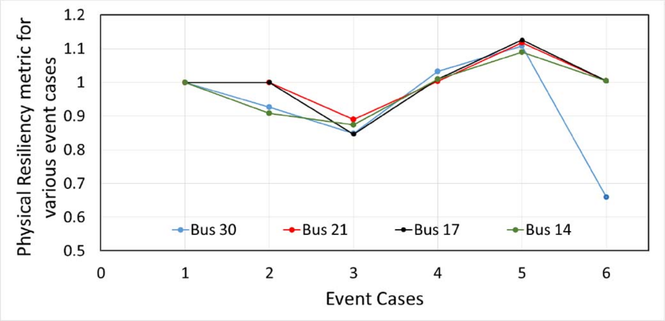

Fig. 8. Variation of resiliency metric at different buses for various event cases. Event Case 1: Normal Operating scenario (base case); Event Case 2: Line $14-15$ is taken out; Event Case 3: Line $2-6$, $6-28$, $10-20$ & $12-16$ are taken out; Event Case 4: Double circuit lines in line $2-5$, $12-15$, $27-28$; Event Case 5: Additional Wind generator at bus 15; Event Case 6: Loss of load at bus 30.

goes down (with respect to the base case). The cases that deteriorate the resiliency include: loss of transmission lines (case 2 and 3), loss of load (case 6). On the other hand, for cases where the system is enhanced using double circuit lines or additional generator, the physical resiliency goes up (with respect to the base case). The cases that enhance the resiliency include: double circuit lines in transmission lines (case 4), additional generator (case 5).

For event case 1, i.e., normal operation of the system, the physical resiliency metric at all buses is equal to 1. In the event case 2, wherein line $14-15$ is taken out from the system, the resiliency metric at buses 14 and 30 reduces to 0.9084 and 0.9261 respectively. On the other hand, the physical resiliency metric at buses 17 and 21 remains almost same. This shows that the outage of line $14-15$ doesn't affect buses 17 and 21. In the event case 3, wherein lines $2-6$, $6-28$, $10-20$ & $12-16$ are taken out, the physical resiliency metric reduces at all the buses as seen from Fig. 8. In case of events 4 and 5, where additional components are built-in the system, it can be observed that the physical resiliency metric improves and helps to increase the resiliency of the system at all buses of the system. In event 6, due to some fault, a part of priority/critical load at bus 30 is shed. This results in significant reduction (due to Loss of Load index at bus 30) of physical resiliency metric at bus 30 to 0.6604, whereas, the physical resiliency metric at all other buses remain same (similar to basecase).

As a case study, a low probability event is studied here for the same 30 bus system as shown in Fig. 7. For this case, it is assumed that bus 5 has a critical/priority load of 40MW and 5 MVAr out of the total 94.2 MW and 19 MVAr load. A severe outage event occurs, resulting in outage of: lines $1-2$, $2-4$, $2-5$, $2-6$, and Gen-2, resulting in outage of Bus 2 in the system. This results in a severe instability condition and a load shedding scheme is initiated to save the system from a collapse. In this study, two different load shedding schemes have been implemented - a) A normal load shedding scheme, wherein resiliency factor is not taken into account; b) An improvised load shedding scheme, wherein resiliency factor is taken into account. These load shedding schemes act as Special Protection Schemes that are triggered in the advent of emergency conditions. The normal load shedding scheme results in a shedding of 74.2 MW of load at bus 5. This results in decrease of physical resiliency at bus 5 of the system to 0.486. But in the case of improvised load shedding scheme, wherein, the system collapse is prevented by shedding a part of load at bus 5 along with shedding of load at bus 7. In this scenario, the physical resiliency at bus 5 is 0.821. The results for this study are shown in Table VI.

TABLE VI
RESILIENCY ANALYSIS OF 30 BUS SYSTEM AT BUS 5 DURING VARIOUS OPERATING CONDITIONS

| | **SPD index** | **MW index** | **MVAr index** | **LOL index** | **Resiliency** |
|---|---|---|---|---|---|
| **Normal operating condition** | 2.664 | 0.696 | 2.727 | 1.000 | 1.000 |
| **Bus 2 outage with normal load shedding scheme** | 0.505 | 0.929 | 2.215 | 0.511 | 0.486 |
| **Bus 2 outage with improvised load shedding scheme** | 0.505 | 0.981 | 2.893 | 1.000 | 0.821 |

## *B. Case Study for Cyber Resiliency*

The IEEE 14 bus test system is taken as a reference for this case study. The cyber resiliency analysis is done for bus 2 as an example. The single diagram for bus 2 is shown in Fig. 9. The substation consists of 6 circuit breakers connecting 4 transmission lines, a load and a generator to the bus.

The IED configuration for this substation is listed in table VII. It can be observed that there are a total of 6 bays in the substation. With reference to the substation automation design in [53], it is considered that there are redundant protection IEDs (one for main protection and other for back-up protection) and only one control IED for each bay. An instance of the security graph is shown in Fig. 10.

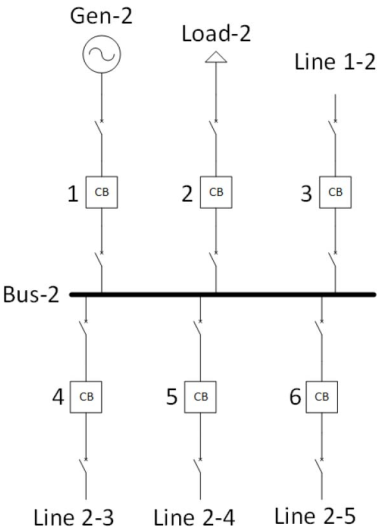

Fig. 9. Single line diagram of substation at bus 2 of IEEE 14 bus system.

TABLE VII
IED CONFIGURATION FOR SUBSTATION-2 OF IEEE 14 BUS SYSTEM

| Name of Bay | Control IEDs | Protection IEDs |
|---|---|---|
| Gen-2 | 1 | 2 |
| Load-2 | 1 | 2 |
| Line 1-2 | 1 | 2 |
| Line 2-3 | 1 | 2 |
| Line 2-4 | 1 | 2 |
| Line 2-5 | 1 | 2 |

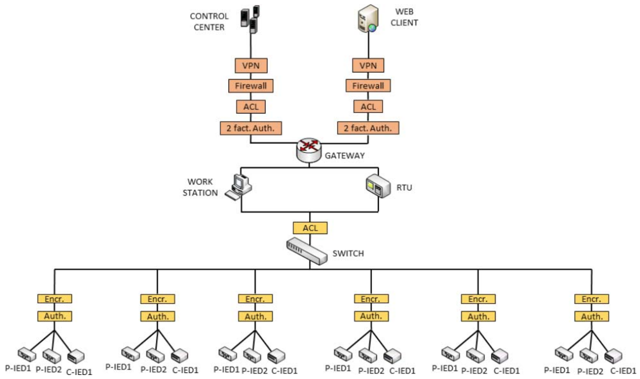

Fig. 10. Security graph.

Two instances of the same substation at bus 2 (A and B) with different security mechanisms deployed in the network. Substation A and B have the security mechanisms as shown in table VIII. It is to be noted here that these pair-wise comparison matrices are an instance for this case study and can be varied based on user/application. The security score for the substation for instances A and B are calculated to be 22.78 and 76.72. The attackability score is calculated based on Eqn. (7) 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. Finally, the cyber-resiliency score is calculated to be 11.55 and 38.52 respectively, with equal weightage for both attackability and security scores.

TABLE VIII
COMPARISON OF SECURITY MECHANISMS DEPLOYED AT DIFFERENT INSTANCES (A AND B) OF SAME SUBSTATION

| | Substation A | Substation B |
|---|---|---|
| **SM1** | Default authentication | Multi-level authentication |
| **SM2** | IDS | SIEM |
| **SM3** | IPS, Traditional firewall | IPS, Improved firewall, VLAN |
| **SM4** | Asymmetric key | Symmetric key |
| **SM5** | Obsolete security mechanism | Regularly patched security mechanism |
| **SM6** | Educational programs | Educational programs, defense in depth approach |

TABLE IX
PAIR-WISE COMPARISON MATRIX FOR DIFFERENT CATEGORIES OF SECURITY MECHANISMS

| | $\mathbf{SM_1}$ | $\mathbf{SM_2}$ | $\mathbf{SM_3}$ | $\mathbf{SM_4}$ | $\mathbf{SM_5}$ | $\mathbf{SM_6}$ |
|---|---|---|---|---|---|---|
| $\mathbf{SM_1}$ | 1 | 1/3 | 1/5 | 1/7 | 3 | 5 |
| $\mathbf{SM_2}$ | 3 | 1 | 1/3 | 1 | 3 | 5 |
| $\mathbf{SM_3}$ | 5 | 3 | 1 | 3 | 5 | 7 |
| $\mathbf{SM_4}$ | 7 | 1 | 1/3 | 1 | 5 | 7 |
| $\mathbf{SM_5}$ | 1/3 | 1/3 | 1/5 | 1/5 | 1 | 3 |
| $\mathbf{SM_6}$ | 1/5 | 1/5 | 1/7 | 1/7 | 1/3 | 1 |

## V. CONCLUSION

The growing inter-dependence of physical power systems on Information Technology (IT) has emphasized the need to study cyber-physical aspects of power systems. In this paper, a novel method for quantifying cyber-physical resiliency is proposed for the transmission electric grid. The cyber-physical resiliency metric is based on both operational and infrastructural components such that these metrics are updated in real-time with changing scenarios. Developed framework can be easily extended for integrating additional factors impacting resiliency. The resiliency analysis approach is tested and validated on different test systems and the results are discussed in detail. Root cause analysis for observed change in resiliency and decision making for enhanced resiliency will be one of the future efforts.

## REFERENCES

[1] *North American Energy Resilience Model*, Dept. Energy, Washington, DC, USA, 2019. [Online]. Available: https://www.energy.gov/sites/prod/files/2019/07/f65/NAERM_Report_public_version_072219_508.pdf

[2] Executive Office of the President, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*. Washington, DC, USA: Council, 2013.

[3] E. D. Vugrin, D. E. Warren, and M. A. Ehlen, "A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane," *Process Safety Progr.*, vol. 30, no. 3, pp. 280–290. 2011.

[4] G. Dondossola, G. Deconinck, F. D. Giandomenico, S. Donatelli, M. Kaâniche, and P. Veríssimo, "Critical utility infrastructural resilience," 2012. [Online]. Available: arXiv:1211.5736.

[5] R. Gustavsson and B. Ståhl, "Self-healing and resilient critical infrastructures," in *Critical Information Infrastructure Security*, R. Setola and S. Geretshuber, eds. Heidelberg, Germany: Springer, 2009, pp. 84–94.

[6] C. Chen, J. Wang, F. Qiu, and D. Zhao, "Resilient distribution system by microgrids formation after natural disasters," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 958–966, Mar. 2016.

[7] P. Bajpai, S. Chanda, and A. K. Srivastava, "A novel metric to quantify and enable resilient distribution system using graph theory and choquet integral," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2918–2929, Jul. 2018.

[8] V. Venkataramanan, A. Hahn, and A. Srivastava, "CP-SAM: Cyber-physical security assessment metric for monitoring microgrid resiliency," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1055–1065, Mar. 2020.

[9] V. Venkataramanan, A. K. Srivastava, A. Hahn, and S. Zonouz, "Measuring and enhancing microgrid resiliency against cyber threats," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 6303–6312, Nov./Dec. 2019.

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

[11] M. Bessani *et al.*, "Probabilistic assessment of power distribution systems resilience under extreme weather," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1747–1756, Jun. 2019.

[12] H. Farzin, M. Fotuhi-Firuzabad, and M. Moeini-Aghtaie, "Enhancing power system resilience through hierarchical outage management in multi-microgrids," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2869–2879, Nov. 2016.

[13] L. Yang, Y. Zhao, C. Wang, P. Gao, and J. Hao, "Resilience-oriented hierarchical service restoration in distribution system considering microgrids," *IEEE Access*, vol. 7, pp. 152729–152743, 2019.

[14] J. Kim and Y. Dvorkin, "Enhancing distribution system resilience with mobile energy storage and microgrids," *IEEE Trans. Smar Grid*, vol. 10, no. 5, pp. 4996–5006, Sep. 2019.

[15] S. Lei, C. Chen, H. Zhou, and Y. Hou, "Routing and scheduling of mobile power sources for distribution system resilience enhancement," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5650–5662, Sep. 2019.

[16] K. Gowtham and A. K. Srivastava, "Resilience of the electric distribution systems: Concepts, classification, assessment, challenges, and research needs," *IET Cyber Phys. Syst. Theory Appl.*, vol. 3, no. 2, pp. 133–143, 2019.

[17] M. Panteli, C. Pickering, S. Wilkinson, R. Dawson, and P. Mancarella, "Power system resilience to extreme weather: Fragility modeling, probabilistic impact assessment, and adaptation measures," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3747–3757, Sep. 2017.

[18] J. Lu, J. Guo, Z. Jian, Y. Yang, and W. Tang, "Resilience assessment and its enhancement in tackling adverse impact of ice disasters for power transmission systems," *Energies*, vol. 11, no. 9, p. 2272, 2018.

[19] R. T. Marsh, *Critical Foundations: Protecting America's Infrastructures: The President's Commission on Critical Infrastructure Protection*. Washington, DC, USA: Commission, 1997.

[20] Z. Bie, Y. Lin, G. Li, and F. Li, "Battling the extreme: A study on the power system resilience," *Proc. IEEE*, vol. 105, no. 7, pp. 1253–1266, Jul. 2017.

[21] D. H. Ryu, H. Kim, and K. Um, "Reducing security vulnerabilities for critical infrastructure," *J. Loss Prevent. Process Ind.*, vol. 22, no. 6, pp. 1020–1024, 2009.

[22] A. A. Creery and E. J. Byres, "Industrial cybersecurity for a power system and SCADA networks—Be secure," *IEEE Ind. Appl. Mag.*, vol. 13, no. 4, pp. 49–55, Jul./Aug. 2007.

[23] M. T. O. Amanullah, A. Kalam, and A. Zayegh, "Network security vulnerabilities in SCADA and EMS," in *Proc. IEEE/PES Transm. Distrib. Conf. Exposit. Asia–Pac.*, Dalian, China, Aug. 2005, pp. 1–6.

[24] G. Li, W. Ju, and D. Shi, "Functional vulnerability assessment of SCADA network," in *Proc. Asia–Pac. Power Energy Eng. Conf.*, Shanghai, China, Mar. 2012, pp. 1–4.

[25] V. Rosato, L. Issacharoff, S. Meloni, D. Caligiore, and F. Tiriticco, "Is the topology of the Internet network really fit to sustain its function?" *Physica A, Stat. Mech. Appl.*, vol. 387, no. 7, pp. 1689–1704, 2008.

[26] R. Sawatari and T. Ohira, "Phase transition in computer network traffic model," *Phys. Rev. E*, vol. 58, p. 193, Nov. 1998.

[27] Y. Jiaxi, M. Anjia, and G. Zhizhong, "Vulnerability assessment of cyber security in power industry," in *Proc. IEEE PES Power Syst. Conf. Exposit.*, Atlanta, GA, USA, Oct. 2006, pp. 2200–2205.

[28] T. Conway, R. M. Lee, and M. J. Assante, "Analysis of the cyber attack on the Ukrainian power grid. Defense use case," Rep., SANS ICS, Washington, DC, USA, 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[29] J. D. McDonald, *Electric Power Substations Engineering*, R. C. Dorf, Eds. Boca Raton, FL, USA: CRC Press, 2016.

[30] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[31] *Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case*, Elect. Inf. Sharing Anal. Center (E-ISAC), Washington, DC, USA, 2016.

[32] A. Nourian and S. Madnick, "A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet," *IEEE Trans. Depend. Secure Comput.*, vol. 15, no. 1, pp. 2–13, Jan./Feb. 2018.

[33] C. S. Holling, "Resilience and stability of ecological systems," *Annu. Rev. Ecol. Systemat.*, vol. 4, no. 1, pp. 1–23, 1973.

[34] C. Perrings, "Resilience and sustainable development," *Environ. Develop. Econ.*, vol. 11, no. 4, pp. 417–427, 2006.

[35] W. N. Adger, "Social and ecological resilience: Are they related?" *Progr. Human Geography*, vol. 24, no. 3, pp. 347–364, 2000.

[36] J. Taft. (2018). *Electric Grid Resilience and Reliability for Grid Architecture*. [Online]. Available: https://gridarchitecture.pnnl.gov/media/advanced/Electric_Grid_Resilience_and_Reliability_v4.pdf

[37] E. Cotilla-Sanchez, P. D. H. Hines, C. Barrows, and S. Blumsack, "Comparing the topological and electrical structure of the north American electric power infrastructure," *IEEE Syst. J.*, vol. 6, no. 4, pp. 616–626, Dec. 2012.

[38] B. A. Carreras, D. E. Newman, I. Dobson, and A. B. Poole, "Evidence for self-organized criticality in a time series of electric power system blackouts," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 51, no. 9, pp. 1733–1740, Sep. 2004.

[39] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the north american power grid," *Phys. Rev. E*, vol. 69, no. 2, 2004, Art. no. 025103.

[40] E. Bompard, E. Pons, and D. Wu, "Extended topological metrics for the analysis of power grid vulnerability," *IEEE Syst. J.*, vol. 6, no. 3, pp. 481–487, Sep. 2012.

[41] Z. Wang, A. Scaglione, and R. J. Thomas, "Electrical centrality measures for electric power grid vulnerability analysis," in *Proc. 49th IEEE Conf. Decis. Control (CDC)*, Atlanta, GA, USA, Dec. 2010, pp. 5792–5797.

[42] V. Rosato, S. Bologna, and F. Tiriticco, "Topological properties of high-voltage electrical transmission networks," *Elect. Power Syst. Res.*, vol. 77, no. 2, pp. 99–105, 2007.

[43] J. Y. Yen, "An algorithm for finding shortest routes from all source nodes to a given destination in general networks," *QuArt. Appl. Math.*, vol. 27, no. 4, pp. 526–530, 1970.

[44] R. Christie. (1993). *Power System Test Case Archive*. [Online]. Available: https://www2.ee.washington.edu/research/pstca/pf14/pg_tca14bus.htm

[45] J.-H. Kim and J.-B. Park, "Generators availability modeling considering planned maintenance outage and demand clustering," in *Proc. Power Eng. Soc. Gen. Meeting*, Montreal, QC, Canada, 2006, p. 7.

[46] P. Lagonotte, J. Sabonnadiere, J.-Y. Leost, and J.-P. Paul, "Structural analysis of the electrical system: Application to secondary voltage control in France," *IEEE Trans. Power Syst.*, vol. 4, no. 2, pp. 479–486, May 1989.

[47] R. Saaty, "The analytic hierarchy process—What it is and how it is used," *Math. Model.*, vol. 9, nos. 3–5, pp. 161–176, 1987.

[48] *Communication Network Solutions for Transmission and Distribution Grids*, Siemens, Munich, Germany, 2016. [Online]. Available: https://assets.new.siemens.com/siemens/assets/api/uuid:8b4809cf50679ccae32f511471c3eb92d064c814/version:1501223616/cgem-160662-communication-network-solutions-16-seiter-row-lowres.pdf

[49] *Power Grid Communications: Solutions for the Energy Sector*, Rad Corp., Feltham, U.K., 2019. [Online]. Available: https://walkerfirst.com/uploads/files/literature/RAD%20Power%20Grid%20Solutions.pdf

[50] R. A. Martin, *Common Weakness Enumeration*, Mitre Corp., McLean, VA, USA, 2007.

[51] T. J. Williams, "The purdue enterprise reference architecture," *Comput. Ind.*, vol. 24, nos. 2–3, pp. 141–158, 1994.

[52] D. E. Bakken, A. Bose, C. H. Hauser, D. E. Whitehead, and G. C. Zweigle, "Smart generation and transmission with coherent, real-time data," *Proc. IEEE*, vol. 99, no. 6, pp. 928–951, Jun. 2011.

[53] *IEC Standard for Communication Network and Systems in Substations*, IEC Standard 61850, 2003.