Modeling Cyber Resilience for Energy Delivery Systems Using Critical System Functionality

Md Ariful Haque[†], Sachin Shetty[†], Bheshaj Krishnappa[‡]
[†]*Computational Modeling and Simulation Engineering, Old Dominion University, Norfolk, VA, USA*
[‡]*Risk Analysis and Mitigation, ReliabilityFirst, Cleaveland, OH, USA*
{mhaqu001, sshetty}@odu.edu[†], bheshaj.krishnappa@rfirst.org[‡]

***Abstract*—In this paper, we analyze the cyber resilience for the energy delivery systems (EDS) using critical system functionality (CSF). Some research works focus on identification of critical cyber components and services to address the resiliency for the EDS. Analysis based on the devices and services excluding the system behavior during an adverse event would provide partial analysis of cyber resilience. To address the gap, in this work, we utilize the vulnerability graph representation of EDS to compute the system functionality under adverse condition. We use network criticality metric to determine CSF. We estimate the criticality metric using graph Laplacian matrix and network performance after removing links (i.e., disabling control functions, or services). We model the resilience of the EDS using CSF, and system recovery curve. We also provide a comprehensive analysis of cyber resilience by determining the critical devices using TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) and AHP (Analytical Hierarchy Process) methods. We present use cases of EDS illustrating the way control functions and services in EDS map to the vulnerability graph model. The simulation results show that we can estimate the resilience metric using different types of graphs that may assist in making an informed decision about EDS resilience.**

***Index Terms*—Energy Delivery Systems, Cyber Resilience, Critical System Functionality, TOPSIS, AHP, Vulnerability Graph.**

I. Introduction

In today's world, with increasingly sophisticated cyber threats, cybersecurity, and cyber resilience are of significant concerns for critical infrastructures (CI). In 2015 attackers used spear-phishing emails to steal credentials in three energy distribution companies of Ukraine and moved laterally through the corporate network and gained access to the supervisory control and data acquisition (SCADA) system [1]. According to E-ISAC [1], the cyberattack incident on the Ukrainian power grid points on the need for building defenders capabilities to confront highly targeted and directed attacks on EDS. The attacks may include utilizing the industrial control systems (ICS) command and control to destroy communication and wiping devices to prevent automated recovery of the system. Thus, there need to develop active cyber defense strategies, and resilient operation plans to survive from a sophisticated attack. Accordingly, there is the urge for modeling cyber resilience analytics for the EDS in a comprehensive manner which would facilitate in developing cost-effective mitigation procedures and defense strategies.

To address the security and resilience, the National Institute of Standards and Technology (NIST) provides security guidelines (Stouffer et al. [2]) for ICS. These guidelines clearly state the need for identifying critical assets, essential ICS services, and control functions within the system. The Cyber Security Evaluation Program within the U.S. Department of Homeland Security's National Cyber Security Division [3] emphasizes on identifying and protecting critical assets and services for having secure and resilient CI. David et al. [4] address resilience for CI by considering the performance of the services provided by individual elements during a disruptive event. Likewise, Herrera and Maennel [5] emphasize on the importance of the identification of essential services and cyber dependencies to address the cybersecurity for Critical Information Infrastructure (CII) systems. Seppänen et al. [6] present a qualitative method for identifying the CI service failure inter-dependencies to assess the impact of cascading failures and cyber resilience. The above works focus the cyber assets and services to evaluate the CI resilience and fail to consider inherent system vulnerabilities in modeling resilience. Thus, the studies lack to provide comprehensive modeling of the system functionality and resilience during a cyberattack incident.

In this work, we use a comprehensive analysis of system functionality for modeling and estimation of cyber resilience for the EDS. We utilize the vulnerability graph model for modeling the EDS IT (Information Technology) and OT (Operational Technology) network. Nodes in vulnerability graph represent EDS IT and OT network devices. IT network consists of application servers, routers, switches, and firewalls, etc. OT network devices include RTU (Remote Terminal Unit), PMU (Phase Measurement Unit), PLC (Programmable Logic Controller), IED (Intelligent Electronic Devices), etc. Throughout the paper, we consider links as logical connections among different devices, which communicate the control functions or services rendered by those devices. We suppose paths as a sequence of services or control functions. We assume the removal of link as disabling the service or deactivating the control function rendered by the particular device.

We determine the critical system functionality using the network criticality metric, which is again computed using the graph Laplacian matrix. We model system recovery nature by utilizing the methods illustrated by Zobel [7]. We derive the cyber resilience metric by using the CSF and the system recovery graph. To identify the critical devices in the EDS IT

978-1-7281-2135-2/19/$31.00 ©2019 IEEE

and OT network, we use TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) and AHP (Analytical Hierarchy Process) methods. TOPSIS is an effective method for ranking problems as illustrated by Hwang [8]. In brief, the contributions of this work are:

- Modeling and drafting critical system functionality
- Modeling and estimation of cyber resilience for EDS using the system recovery behavior during an adverse event
- Formulating network, device, control functions, and attack paths criticality
- Incorporating CVSS exploitability and impact metrics in the vulnerability graph model for resilience assessment.

The rest of the paper is organized as follows. Section II provides related works that use similar approaches to estimate network criticality, critical system functionality, and resilience. Section III maps the EDS use cases to the proposed analysis and discusses the vulnerability graph model. Section IV presents the modeling approaches for resilience metrics. Section V presents simulation results and discussions. Section VI concludes the work by discussing future research directions.

II. Related Work

In the context of cyber-physical systems, we consider resilience as the ability of the system to defend against cyberattack incidents and maintain an acceptable level of performance by preserving critical system functionality, and timely restoring to the pre-incident level of quality of services. Several pieces of research address the cyber resiliency for EDS. In this paper, we limit our focus on the research related to critical infrastructures resilience assessment.

Researchers use criticality-based analysis in evaluating asset criticality in CI networks, power grid, cyber defense applications, etc. Timashev [9] addresses the reliability, resilience, and safety of infrastructures exposed to cyberattacks. Anya and Kang [10] focus criticality in proposing defense strategies to prevent cyberattacks on the CI. Likewise, Ren and Sovacool [11] utilize the criticality metrics for quantifying, measuring, and developing strategies for energy security. Moreover, Shen and Tang [12] propose a robust estimation procedure for the power-law distribution for enhancing resilience analysis of power systems. Amin [13] addresses challenges for reliable, resilient, and secure cyber-physical power and energy systems. Haque et al. [14] present a similar discussion on challenges in deriving cyber-physical systems resilience analytics. These works address cyber resiliency from criticality standpoint but failed to establish the relationship of the system behavior during a cyberattack incident to the resilience metric.

Farnaz et al. [15] discuss the cyber-related risk assessment and critical asset identification in power grids by utilizing a mixture of AHP and (N-1) contingent analysis. Likewise, Gómez et al. [16] describe the design and the implementation of a process of asset criticality analysis for distribution network service providers. Reza et al. [17] believe that the concept of a power system's cyber-physical resilience centers around maintaining critical functionality of the system backbone in the presence of unexpected extreme disturbances. Vugrin et al. [18] propose infrastructure resilience assessment techniques through control design. Haque et al. [19] propose a qualitative resilience assessment method for industrial control systems.

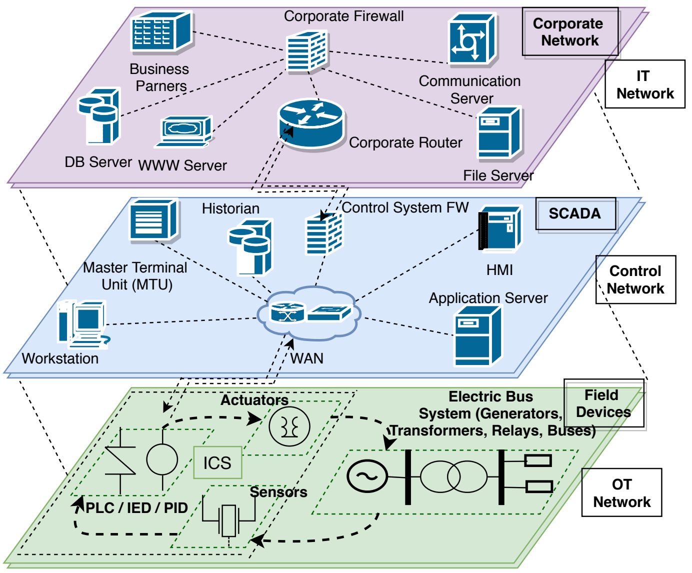


Fig. 1. EDS IT, SCADA, and OT network.

Most of the above research propose different techniques to evaluate resilience by using asset criticality. Some works determine criticality by considering individual influence in the network. Some other works suggest risk-tolerant strategies using criticality metrics. Although some of the works mention critical functionality to address cyber resilience, there is a lack of modeling system functionality for EDS during an attack event in the current research. NIST [2] also articulates the need for maintaining system functionality during adverse conditions. Thus, there is a need for comprehensive system functionality modeling to estimate cyber resilience. That implies examining network architecture (topology), control functions, vulnerabilities, and potential impacts due to a cyber incident. In this work, we primarily focus on the modeling of CSF to estimate cyber resilience for EDS. We also derive the criticality metrics for devices, control functions, attack paths, and overall EDS IT and OT network.

III. Preliminaries

In this section, we present the details of the vulnerability graph and EDS use cases that we want to formulate.

A. EDS Use Cases

Fig. 1 illustrates a hierarchical view of the EDS network consisting of IT , SCADA, and OT. In this work, we focus on the IT, SCADA and OT network components and the services and control functions running on these devices. The OT network is consisting of ICS devices such as RTU, PLC, PMU, IED, etc. SCADA network consists of HMI (Human Machine Interface), MTU (Master Terminal Unit), and other application servers. Based on Fig. 1, we illustrate the following use cases which we model in the consecutive sections.

***Use Case I** (Critical System Functionality (CSF)):* The sensors in the EDS OT network send the measurements from different locations, such as substation buses, transmission lines, etc., to the control center using the SCADA system. The control center utilizes these measurements to determine the state of the power system and generate new control commands to be issued, if needed, to reach the desired state. The commands from the control center are reissued over the SCADA system to the field devices through the actuators. During a cyberattack incident, the intruder may successfully disable the associated control functions or control devices, and thus, the sensor data are not available from those malfunctioned devices. This condition of loss of command and control on the field devices may lead the OT network to perform in degraded mode but not entirely out of operation because of redundancy in the physical devices or logical connections. The CSF indicates the minimal operational level that is maintained by the system during an adverse event. We compute the CSF in section IV by generating new vulnerability graph without the removed edges (i.e., without the out of service control functions).

***Use Case II** (Critical Control Functions):* The RTU, PLC, PMU, IED, and other sensors in the OT network provides specific control functions for the regular operation of the EDS. We model these functions as the links between the devices because the links control the logical connections among devices. Thus, taking out of a link in the EDS vulnerability graph model is interpreted as a loss of the specific system function (e.g., feedback control, loss of sensor data, etc.) provided by the corresponding device. Similarly, a path is consisting of a sequence of links which in other terms construed as a combination of the control functions provided by those devices falling in the chain of logical connections.

***Use Case III** (Critical Devices):* Depending on the network topology, security policy, and associated loads on the electrical buses, some of the control devices in the OT network are more critical from cyber perspectives than the others. Thus, by representing the devices in SCADA, IT, and OT by nodes, and the logical connectivity by the edges in the vulnerability graph we derive the critical assets (hosts or devices) that are prone to cyberattacks based on the assets' vulnerabilities. We compute the device criticality metric in section IV by using TOPSIS and AHP.

B. Vulnerability Graph Model

A vulnerability graph is a directed weighted graph $G = (N, E, W)$ where N is the finite set of nodes (or vertices), $E \subseteq N \times N$ is the set of graph links or edges, and W is the weight matrix of the graph. If an edge $e = (i, j)$ connects two nodes i and j, then the nodes i and j are said to be adjacent to each other. A path in a graph is defined as a walk from a source node to a destination node without repeated nodes. An adjacency matrix A of a graph $G = (N, E, W)$ with $|N| = n$ is an $n \times n$ matrix, where $A_{ij} = W_{ij}$, if $(i, j) \in E$ and $A_{ij} = 0$ otherwise. The weights W_{ij} between the edge (i, j) is coming from the CVSS exploitability score of the node j. That is why we call the graph G as a vulnerability graph.

*1) **Network Topology and Connectivity**:* In a network such as EDS, there are specific security policies (e.g., firewall rule-sets) to follow. In the EDS or ICS, as per the NIST guidelines [2], the message or protocol level communications among SCADA and field devices are done through ICS firewalls having specific rule-sets. The adjacency matrix that we have defined above is representing the network topology and connectivity in our vulnerability graph model.

*2) **Control Functions**:* We define the control funtions (CFs) as the logical connections that carry the data from the fielded devices to SCADA and control commands from SCADA to the fielded devices. CFs perform the specific tasks (such as voltage regulation, phase angle adjustment, etc.). Mathematically, we denote a control function $C_f(i, j)$ between node i & j as $\{C_f(i, j) = e(i, j) \mid \exists\ e(i, j) \in E,\ A_{ij} \neq 0\ \&\ W_{ij} > 0\}$, and the weight W_{ij} represent the exploitability of the control function $C_f(i, j)$. We do not consider the utilization of the control function in this model yet but plan to include in the future work.

*3) **Exploitability and Impact Metrics**:* CVSS [20] defines the exploitability and impact metrics for every known vulnerability. The exploitability metric comprises three base metrics: access vector A_V, access complexity A_C, and access authentication A_U. Similarly, the impact metric consists of three base metrics: confidentiality impact I_C, integrity impact I_I, and availability impact I_A. We compute the exploitability and impact of a vulnerability i as in eq. (1) and (2) [20].

$$ES_i = 20 \times A_V^i \times A_C^i \times A_U^i \tag{1}$$

$$IS_i = 10.41 \times (1 - (1 - I_C^i)(1 - I_I^i)(1 - I_A^i)) \tag{2}$$

The exploitability score (ES) is on a scale of $0 \sim 10$, and the higher value indicates higher exploit capability by a cyber attacker. Similarly, the higher the impact score (IS), the higher is the possible damage an attacker may cause upon exploiting the vulnerability.

*4) **Edge Weight Computation**:* We compute the edge weights of the vulnerability graph by using eq. (1), and define the weight matrix as below.

$$W_{ij} = \begin{cases} ES_j & \text{if } (i, j) \in E \\ 0 & \text{otherwise, i.e., if } (i, j) \notin E \end{cases}$$

*5) **Betweenness Centratlity (BC)**:* BC quantifies the number of times a node acts as a bridge along the shortest path between two other nodes. BC is a crucial graph-theoretic metric which indicates the possible criticality of a node, i.e., the possibility of attack progression through a node. The betweenness centrality of a node n, B_n is the fraction of the shortest paths going through n and is given by eq. (3).

$$B_n = \sum_{s \neq n \neq t} \frac{\sigma_{st}(n)}{\sigma_{st}} \tag{3}$$

Where σ_{st} is the total number of shortest paths from node s to node t and $\sigma_{st}(n)$ is the number of those paths that pass-through node n.

*6) **Katz Centratlity (KC):*** KC measures the number of all nodes that can be connected through a path, while the contributions of distant nodes are penalized. Haque et al. ([21], [22]) define asset values by the importance of the information contained by the network component, which is also dependent on the predecessor nodes importance. Thus, the asset value that is addressed by Haque et al. [21] to rank critical nodes can be formalized by KC. Mathematically, the KC of node i is defined as eq. (4), where α is an attenuation factor and $0 \leq \alpha \leq 1$.

$$C_{Katz}(i) = \sum_{k=1}^{\infty} \sum_{j=1}^{n} \alpha^k (A^k)_{ji} \tag{4}$$

We utilize BC and KC only in the identification of the critical devices and control functions. We do not use BC and KC directly in resilience assessment.

IV. System Functionality, Resilience, and Criticality Metrics

This section presents the central analytics of this work. We provide the mathematical formulations of critical system functionality, resilience, device, and control functions criticality metrics in the following subsections by following a top-down approach.

A. Critical System Functionality (CSF)

Reza et al. [17] describe resilience as a multidimensional property of the system, which requires managing disturbances originating from physical component failures, cyber component malfunctions, and cyberattacks. The authors also define CSF as maintaining critical functionality of the system in the presence of unexpected extreme disturbances. Haque et al. [23] propose a way to evaluate essential service functionality using a qualitative approach. Bharali and Baruah [24] define the average network functionality using the network criticality metric and considering random failures. We extend the analysis of Bharali and Baruah [24] for the case of random cyber-attacks on the EDS. We assume removing certain links by a cyberattack incident as deactivating some control functions or services which the attacker achieves by eliminating the logical connections. Here we treat the average network functionality metric as the critical system functionality. The CSF is the level of system functionality maintained by the EDS in case of an adverse incident (i.e., after disabling some control functions, or services).

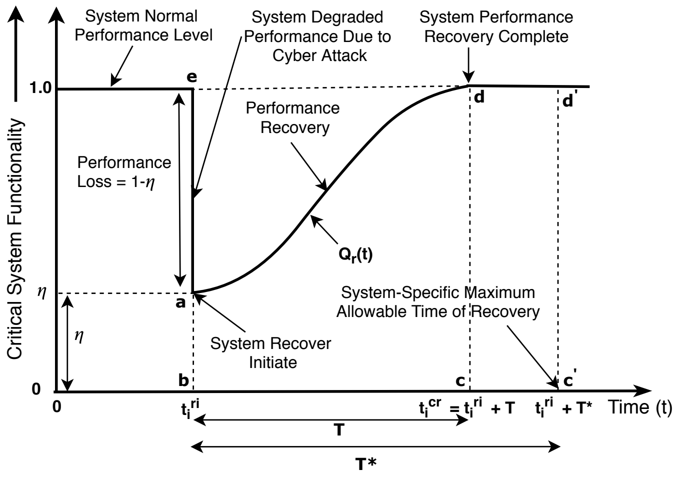


Fig. 2. System performance curve during a cyberattack incident i on EDS.

Let G be the original graph, and $G \backslash e$ be the graph obtained by removing the edge e, then τ and τ_e be the network criticality of G and $G \backslash e$. Then the critical system functionality is defined by eq. (5).

$$\eta = 1 - \frac{1}{m} \sum_{e \in E} \left[H^+(\tau_e - \tau)\frac{\tau}{\tau_e} + H^-(\tau_e - \tau)\frac{\tau}{\tau_e + \frac{2n}{\mu}} \right] \tag{5}$$

Where m is the number of edges in G, μ is the smallest non-zero eigenvalue of G, $H^+(x) = 1$ if $x \geq 0$ and 0 otherwise, and $H^-(x) = 1$ if $x < 0$ and 0 otherwise. For a connected graph G, $\mu = \mu_1$ which is the algebraic connectivity of G and $0 \leq \eta \leq 1$. Thus, η indicates the system functionality of the EDS under adverse cyber events, and a higher value of η means a higher level of system functionality. We compute network criticality τ in subsection IV-C.

B. Cyber Resilience Metric

Dakota et al. [25] define bulk power system resilience as the safeguarding of the critical system functionality when subject to perturbations and restoration after outages. We estimate the cyber resilience for the EDS by utilizing the system recovery curve as in Fig. 2 and using critical system functionality. The nature of the recovery behavior of a system during an adverse event is typically non-linear and is a function of the system under consideration (S), duration of recovery (T), recovery rate (r), time (t), and the functionality level (η) maintained which we express as $Q_r(t) = f(S, \eta, r, T, t)$. Zobel [7] addresses the recovery behavior and proposes several functional forms to model the recovery over time. In this work, we utilize the inverted exponential functional form of the recovery curve, which seems suitable to model the resilience for the EDS. We model the time-dependent system recovery behavior $Q_r(t)$ by following the eq. (6) of Zobel [7] to demonstrate quantitative resilience metric under adverse events where loss of performance $=1 - \eta$ and $0 \leq \eta \leq 1$.

$$Q_r(t) = (1-\eta)\left(1 - \mathrm{e}^{\left(-\frac{\left(T-(t-{t_i}^{ri})\right)ln(n)}{T}\right)} + \frac{(T-(t-{t_i}^{ri}))}{nT}\right) \tag{6}$$

Here, t_i^{ri}= time of recovery initiate, and t_i^{cr} = time of complete recovery of system functions for attack incident i. The period of recovery is $T = t_i^{cr} - t_i^{ri}$. The parameter n defines the level of concavity inherent in the inverted exponential curve.

In Fig. 2, T^* is the system-specific maximum allowable time for the recovery to occur which is selected by the decision makers as the acceptable time within which the system must recover to be considered as operational (i.e., not abandoned). The area formed by the points e-a-d is the amount of system functionality losses over time due to the cyberattack incident i. The area enclosed by the points a-b-c′-d′ is the area of system resilience. To compute the resilience metrics, we first compute the area enclosed by the points e-a-d, which is as follows:

$$A_{e-a-d} = (1-\eta) \int_{t_i^{ri}}^{t_i^{ri}+T} \left(1 - \mathrm{e}^{\left(-\frac{\left(T-(t-{t_i}^{ri})\right)ln(n)}{T}\right)} + \frac{(T-(t-{t_i}^{ri}))}{nT}\right) dt$$

Simplifying the above equation, we find the following reduced form as in eq. (7).

$$A_{e-a-d} = (1-\eta)T\Big[1 - \frac{n-1}{nln(n)} + \frac{1}{2n}\Big] \tag{7}$$

From Fig. 2, we find the area of e-b-c′-d′ is $1 * T^* = T^*$. We find the area of e-a-d by using eq. (7). Thus, the cyber resilience of the EDS is the area under the curve enclosed by the points a-b-c′-d′ over period T^* as given in eq. (8).

$$\xi = \frac{1}{T^*}\left[T^* - (1-\eta)T\left(1 - \frac{n-1}{nln(n)} + \frac{1}{2n}\right)\right] \tag{8}$$

The term $\left(1 - \frac{n-1}{nln(n)} + \frac{1}{2n}\right)$ is a constant term for specific n, and is denoted by β. Thus, eq. (8) becomes $\xi = \frac{1}{T^*}\big[T^* - (1-\eta)T\beta\big]$.

C. Network Criticality

Bharali and Baruach [24], and Ali and Garcia [26] propose graph-based network criticality metric. We apply the same metric here to measure the criticality of the overall EDS network. We use the Moore-Penrose inverse of the Laplacian matrix L to compute the network criticality τ. As we are using the directed weighted graph, the Laplacian matrix L is defined as below following Chung Fan [27] where P is the transition matrix of the graph, Φ is a matrix with the Perron vector of P in the diagonal and zeros elsewhere.

$$L = I - \left(\Phi^{\frac{1}{2}} P \Phi^{\frac{-1}{2}} + \Phi^{\frac{-1}{2}} P^T \Phi^{\frac{1}{2}}\right)/2 \tag{9}$$

Another way to derive L is by using the normalized graph Laplacians L_{sym} and random walk Laplacian L_{rw}, as below.

$$L_{sym} = D^{\frac{-1}{2}} L D^{\frac{-1}{2}} = I - D^{\frac{-1}{2}} W D^{\frac{-1}{2}}$$

$$L_{rw} = D^{\frac{-1}{2}} L_{sym} D^{\frac{1}{2}}$$

where D is a diagonal matrix formed by the degree of the nodes in the vulnerability graph and defined as $D = diag(d_1, d_2, ..., d_m)$. Here $d_i = \sum_{j=1}^{m} W_{ij}$. We find the Moore-Penrose inverse of the Laplacian matrix L, L^+ by following Bernstein [28] as we illustrate in eq. (10).

$$L^+ = \left(L + \frac{J}{n}\right)^{-1} - \frac{J}{n} \tag{10}$$

Where J is an $n \times n$ matrix whose entries are all equal to 1. Finally, we define the network criticality τ by eq. (11).

$$\tau = 2n * trace(L^+) \tag{11}$$

Here, n is the number of nodes, L^+ is the Moore-Penrose inverse of the Laplacian matrix L, and $trace(L^+) = \sum_{i=1}^{n}(L^+)_{ii}$. The larger value of τ indicates the network is more vulnerable from the exploitability perspective. We find the normalized network criticality from eq. (12).

$$\hat{\tau} = \frac{2 * trace(L^+)}{n(n-1)} \tag{12}$$

D. Critical Device Identification

Determining the network component or device criticality is a multi-criteria decision analysis (MCDA) problem. Haque et al. [21] identified some of the crucial parameters for ranking the critical nodes in an EDS network from cyberattack perspective using the vulnerability graph model, but the application of the MADM (Multiple-Attribute Decision Making) is not precise. This paper addresses the gap by utilizing TOPSIS and AHP to determine the criticality metrics of a device or network element.

*1) **Parameters**:* It is possible to consider N parameters to compute the device criticality metric. We have considered four parameters to assess the criticality of each device of the EDS in the vulnerability graph model: (1) device's asset value (modeled by Katz centrality (KC)), (2) betweenness centrality (BC), (3) attack exploitability, and (4) attack impact. The attack exploitability and attack impact of a device are computed using eq. (1) and (2). The BC and KC are found using eq. (3) and (4). The explanations of criticality, asset value, exploitability, and attack impact can be found in [21].

*2) **TOPSIS Method for Device Criticality Assessment**:* The Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) (Hwang et al. [8]) builds on the concept that the chosen alternative should have the shortest geometric distance from the positive ideal solution and the longest geometric distance from the negative ideal solution. Anya and Kang [10] also use TOPSIS to determine the device criticality. Here, we briefly present the steps involved in the TOPSIS method.

Step I: We form an $m \times n$ matrix with m criteria (parameters) and n alternatives (nodes/devices), with the intersection of each criteria and alternative contains a value of x_{ij}, where C_m and A_n are the mth criteria and nth alternative.

$$X_{m\times n} = \begin{array}{c} \\ C_1 \\ C_2 \\ ... \\ C_m \end{array} \begin{array}{c} \begin{array}{cccc} A_1 & A_2 & ... & A_n \end{array} \\ \begin{bmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ ... & ... & ... & x_{3n} \\ x_{m1} & x_{m2} & ... & x_{mn} \end{bmatrix} \end{array}$$

Step II: We normalize the matrix $X_{m\times n}$ to form another matrix $R_{m\times n} = (R_{ij})_{m\times n}$ using the following normalization.

$$R_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m}(x_{ij})^2}}$$

Step III: We compute the weighted normalized decision matrix T as below. The weights can be calculated using AHP, as we illustrate in the next subsection.

$$T = (t_{ij})_{m\times n} = (w_i R_{ij})_{m\times n}, j = 1, 2, .., n$$

Step IV: We determine the worst alternative A_w and the best alternative A_b.

$$A_w = \{\langle \max(t_{ij}|j = 1, 2, ..., n|i \in I_-\rangle, \\ \langle \min(t_{ij}|j = 1, 2, ..., n|i \in I_+\rangle\} = \{t_{wi}|i = 1, 2, ..., m\}$$

$$A_b = \{\langle \min(t_{ij}|j = 1, 2, ..., n|i \in I_-\rangle, \\ \langle \max(t_{ij}|j = 1, 2, ..., n|i \in I_+\rangle\} = \{t_{bi}|i = 1, 2, ..., m\}$$

Where we denote the criteria having a positive impact by I_+=$\{i = 1, 2, ..., m|i\}$ and the criteria having a negative impact by I_-=$\{i = 1, 2, ..., m|i\}$.

Step V: We compute the L2-distance between the target alternative j and the worst condition A_w.

$$d_{iw} = \sqrt{\sum_{i=1}^{m}(t_{ji} - t_{wi})^2}, j = 1, 2, ..., n$$

The distance between the alternative j and the best condition A_b is:

$$d_{jb} = \sqrt{\sum_{i=1}^{m}(t_{ji} - t_{bi})^2}, j = 1, 2, ..., n$$

Where d_{jw} and d_{jb} are L2-norm distances from the target alternative i to the worst and best conditions, respectively.

Step VI: Finally, we compute the criticality of alternative j (node j / device j) as below:

$$\eta_j = \frac{d_{jw}}{d_{jw} + d_{jb}}, 0 \leq \eta_j \leq 1, j = 1, 2, ..., n \quad (13)$$

Using the device criticality metric it is possible to identify the critical IT and OT devices.

*3) **Criteria Weights Using AHP**:* In AHP, the pairwise comparisons of m criteria with each other form a matrix C of dimension $m \times m$. Each entry in C denoted by C_{ij} represents the subjective comparison between criteria C_i and C_j. The pairwise comparison matrix C is given by the below matrix where $C_{ij} = \frac{1}{C_{ji}}$.

$$C = \begin{bmatrix} 1 & C_{12} & ... & C_{1m} \\ \frac{1}{C_{12}} & 1 & ... & C_{2m} \\ ... & ... & ... & ... \\ \frac{1}{C_{1m}} & \frac{1}{C_{2m}} & ... & 1 \end{bmatrix}$$

We find the normalized matrix C_N from C by using the equations below where $C_N(i,j) = \frac{C_{ij}}{\sum_{i=1}^{m} C_{ij}}$.

$$C_N = \begin{bmatrix} C_N(1,1) & C_N(1,2) & ... & C_N(1,m) \\ C_N(2,1) & C_N(2,2) & ... & C_N(2,m) \\ ... & ... & ... & ... \\ C_N(m,1) & C_N(m,2) & ... & C_N(m,m) \end{bmatrix}$$

We compute the weights of the criteria from the normalized matrix C_N, which are the normalized right eigenvector of the pairwise comparison matrix C.

$$w = \begin{bmatrix} w_1 \\ w_2 \\ ... \\ w_m \end{bmatrix}$$

where, $w_i = \frac{1}{m}\left(\sum_{j=1}^{m} C_N(ij)\right)$. To check the consistency of the pairwise comparison, we compute the consistency ratio, CR by using $CR = \frac{CI}{RI}$, where RI is the random index, and CI is the consistency index. We calculate CI by utilizing the principle eigenvalue λ_{max} as given in the below equation:

$$CI = \frac{\lambda_{max} - 1}{m - 1}$$

where again we compute λ_{max} by

$$\lambda_{max} = \sum_{j=1}^{m}\left(\sum_{i=1}^{m} C_{ij}\right) * w_j$$

We find the value of RI in Table 6 of [29] by Thomas Satty. We accept the comparison if $CR \leq 0.1$.

E. Critical Control Functions

In the vulnerability graph model, the edges represent the logical connections which carry the control functions (i.e., control commands) among the OT devices. Control function (CF) criticality indicates the extent of the exploitability of the CF compared to its neighboring CFs (i.e., neighboring links in the vulnerability graph). We define the betweenness of the control function $C_f(i,j)$, b_{ij} as in eq. (14).

$$b_{ij} = \sum_{s\in n, t\in n} \frac{\sigma_{st}(i,j)}{\sigma_{st}} \quad (14)$$

where, σ_{st} is the number of shortest paths from the node s to t, and $\sigma_{st}(i,j)$ is the number of shortest paths from s to t that pass through edge (i,j). We define the criticality of the control function $C_f(i,j)$ as the betweenness of the link (i,j) over its weight as in eq. (15) [26]:

$$\eta_{ij} = \frac{b_{ij}}{W_{ij}} \quad (15)$$

We find the edge weight W_{ij} from the weight matrix computed before. We present two other cyber metrics related to control functions in the below subsections.

*1) **Control Function Path Criticality:*** The path criticality metric indicates the extent of the exploitability of an attack path where the path represents a sequence of control functions. We compute the control path criticality metric by dividing the sum of the link criticalities that form the shortest path from a source node s to target node t by the number of links that construct the shortest path. Mathematically,

$$\eta_{P_{st}} = \frac{\sum_{i,j \in P(st)} \eta_{ij}}{|P_{(st)}|} \tag{16}$$

$P(st)$ is the set of the links that form the shortest path from node s to t, and $|P(st)|$ is the cardinality of $P(st)$.

*2) **Control Function Exploit Attractivity:*** The exploit attractivity indicates the attacker attractiveness on exploiting the control function based on its exploitability score. Mathematically, we define the exploit attractivity of a control function as below:

$$p(l) = \frac{W_l}{\sum_{e \in A^o(j)} W_e} \tag{17}$$

Where $l = C_f(i,j)$ is the control function consisting of edge (i,j), W_l is the weight of $C_f(i,j)$, $A^o(j)$ is the set of edges attached to node j, W_e is the weight of CF/edge e.

V. Simulation Results And Discussion

We present here simulation results for an arbitrary EDS network using the vulnerability graph given in Fig. 3. The vulnerability graph is the model representation of the EDS network. We provide stochastic simulation results for randomly generated Watts-Strogatz small-world graph, and Erdös-Rényi graph to simulate the best case and the worst-case scenarios using python NetworkX module. We also present the device, control functions, and attack path criticality metrics following the same sequence for the simulation discussion as we illustrate the EDS use cases.

A. Critical System Functionality and Cyber Resilience

Sample Network Simulation: For the sample vulnerability graph of Fig. 3, we plot the average CSF (η) and resilience (ξ) by sequentially removing random number of links starting from 1 to 10 out of 15 as in Fig. 4a. We present the results for different values of concavity (n) for the recovery graph. With the removal of the links, both η and ξ drops which illustrates the efficacy of the model. In other terms, removal or blockage of control functions due a cyber incident has negative impact on both η and ξ. Fig. 4b shows the deviation of η and ξ from normal with the increasing fraction of link removal.

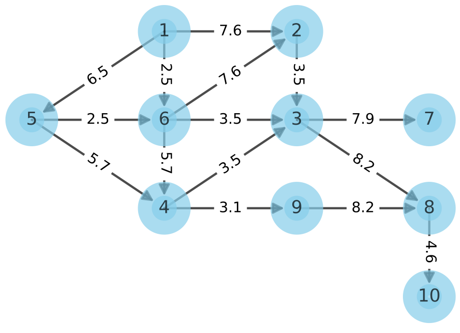
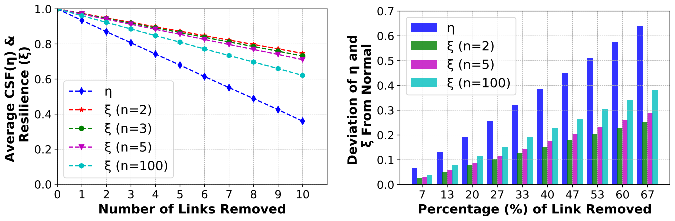


Fig. 3. Sample vulnerability graph representation of EDS.



(a) η and ξ vs. number of links removed

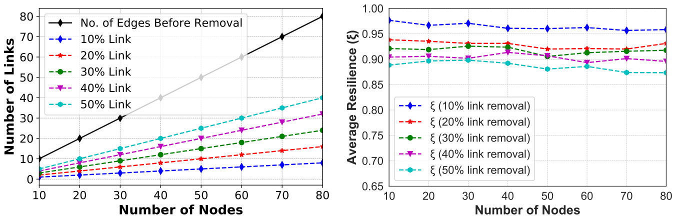
(b) Deviation of η and ξ vs. fraction of links removed

Fig. 4. CSF (η) and cyber resilience (ξ) for the sample network.

Stochastic Network Simulation: We have used two different graphs: Watts-Strogatz small-world (WS) graph and Erdös-Rényi (ER) graph with a large number of nodes for evaluating the behavior of the removal of a large number of edges on cyber resilience (ξ) and scalability. In the WS graph, two nodes are connected by a single edge between them, whereas in the ER graph, every node is having connections to every other node. Thus, WS is a simple network, and ER is a complex network. For the WS graph, we use the edge rewiring probability of 0.05, and for the ER graph (fast_gnp_random_graph in python NetworkX) we use the probability for edge creation of 1.0. We use random edge weights and Monte-Carlo simulation to compute average resilience.

Fig. 5a and 6a show the number of edges that we have removed, and Fig. 5b and 6b show the average resilience for the WS and ER graph respectively. We find that for a significant percentage of edge removal, the resilience drops more compared to the smaller percentage of edge removal. For the case of WS, the value of ξ is between 0.975∼0.875 after removing a significant amount (10%∼50%) of edges, and the same for ER is 0.95∼0.7. Thus, we can conclude that resilience could drop significantly due to the removal of a large fraction of the edges in case of a complex network. We can interpret the result as taking a large number of control functions out of normal operation due to a cyberattack would impact the resilience of the EDS to a significant extent.

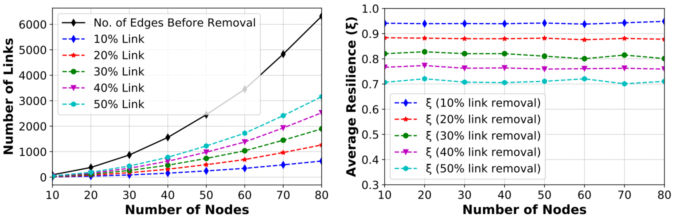
Resilience Histogram From Stochastic Simulation: Fig. 7a and 7b represent the histogram and density plot for the average



(a) Number of links vs. number of nodes (WS graph)

(b) Average resilience (ξ) vs. number of nodes (WS graph)

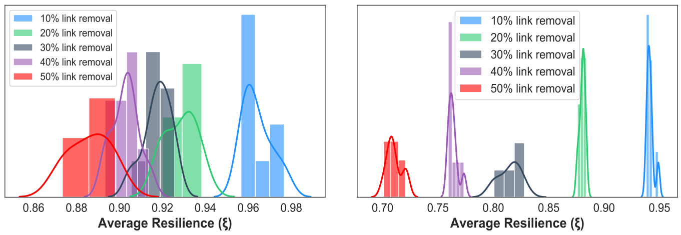
Fig. 5. Number of links removed vs. average resilience (ξ) using Watts-Strogatz small-world (WS) graph.



(a) Number of links vs. number of nodes (ER graph)

(b) Average Resilience (ξ) vs. number of nodes (ER graph)

Fig. 6. Number of links removed vs. average resilience (ξ) using Erdös-Rényi (ER) graph.



(a)

(b)

Fig. 7. Histogram & density plot of average resilience (ξ) for (a) Watts-Strogatz (WS) and (b) Erdös-Rényi (ER) graph

resilience for the simulation that we provide previously. For the WS, we found the average resilience is overlapping in some area between 0.85∼0.95, but for the ER, we have a clear distinction in the resilience area for different percentage of link removal. The more the links or control functions are removed, the less is the resilience value that we achieve. The results show that we can predict the resilience by estimating the impact of attacks on the fraction of control functions.

B. Critical Device Simulation

We provide here the illustrations of TOPSIS for the devices (nodes) 2, 3, 4, 5, 6, and 8 only from Fig. 3 because of space constraints. Table I shows the weights of the criteria and the parameter values of the nodes (devices). Table II shows the corresponding TOPSIS computation. The bold italic underline value is the maximum of the criteria, and bold only is the minimum of the criteria. We find that based on the arbitrary impact and exploitability values and the network model in Fig. 3, the most critical devices are 8 and 6, and the least critical one is 5, considering node 10 as the target.

C. Link and Attack Path Criticality Simulation

TABLE I
DEVICE CRITICALITY ASSESSMENT PARAMETERS

		Device					
Parameter	w_c	2	3	4	5	6	8
Exploitability	0.25	7.6	3.5	5.7	6.5	2.5	8.2
Impact	0.5	5.5	7.2	6.9	2.3	8.9	6.7
Betweenness C.	0.15	0.027	0.185	0.074	0.0138	0.078	0.097
Katz Centrality	0.1	0.327	0.366	0.329	0.294	0.324	0.334

TABLE II
TOPSIS DEVICE CRITICALITY METRICS

	Device (j)					
Parameter	2	3	4	5	6	8
Exploitability	1.9	0.875	1.425	1.625	**0.625**	***2.05***
Impact	2.75	3.6	3.45	**1.15**	***4.45***	3.35
Betweenness C.	0.00405	***0.02775***	0.0111	**0.00207**	0.0117	0.01455
Katz Centrality	0.0327	***0.0366***	0.0329	**0.0294**	0.0324	0.0334
d_{jw}	2.0459	2.4629	2.4352	1.0000	3.3000	2.6212
d_{jb}	1.7068	1.4502	1.1794	3.3274	1.4251	1.1001
η_j	0.5452	0.6294	0.6737	0.2311	**0.6984**	**0.7044**

TABLE III
CONTROL FUNCTIONS CRITICALITY METRICS

$CF/Link(i,j)$	η_{ij}	$CF/Link(i,j)$	η_{ij}
(1, 2)	0.00434	(5, 4)	0.01039
(1, 5)	0.00289	**(5, 6)**	**0.01629**
(1, 6)	**0.01776**	(6, 2)	0.00292
(2, 3)	**0.01903**	**(6, 3)**	**0.02434**
(3, 7)	0.00843	(6, 4)	0.00584
(3, 8)	0.014	**(8, 10)**	**0.01932**
(4, 3)	0.0148	(9, 8)	0.00497
(4, 9)	0.0203		

Table III shows the link criticality for the sample vulnerability graph. Thus, it is possible to focus on the critical links (in bold letters) as those links are having higher values than others and are more exploitable from a cyber perspective. Table IV shows the attack path criticality metrics for all the shortest paths from source node 1 to target node 10. The control path (1, 6, 3, 8, 10) is the shortest path from the source node 1 to target node 10 using Dijkstra algorithm and have larger path criticality between the two shortest paths.

VI. Conclusion and Future Plan

In this work, we address the research gap regarding the relationship between cyber resilience and system behavior during a cyberattack incident. We model the cyber resilience for the EDS network by using the critical system functionality during a cyberattack incident. We provide mathematical formulations of system behavior under adverse condition, cyber resilience, and the criticality metrics for the devices, control functions, and overall network in a comprehensive manner. In the simulation discussion section, we present the critical system functionality and the cyber resilience for different types of graphs, which illustrates the applicability of the model in different network topology scenarios. Thus, the proposed model would help researchers in this field to make more informed decisions by analyzing the system functionality and cyber resilience for the EDS.

In the future, we plan to extend the research and derive a cost-effective cyber mitigation model for the EDS, considering the network topology, devices, control functions,

TABLE IV
CONTROL PATHS CRITICALITY METRICS

Shortest Path (Source=1, Target=10)	$\sum EdgeExploitability$	$\eta_{P_{st}}$
(1 → 2 → 3 → 8 → 10)	23.9	0.014172
(1 → 6 → 3 → 8 → 10)	18.8	**0.018855**

and vulnerabilities. The mitigation model would guide in developing remediation strategies and countermeasures to face the potential cyber threats on the EDS and protect and manage EDS efficiently from cyber intruders by getting a good understanding of the risk and resilience from the proposed analyses. We also plan to include the impact of the control functions in the future model as different control functions have a different level of utilization.

Acknowledgment

This material is based upon work supported by the Department of Energys Office of Cybersecurity, Energy Security, and Emergency Response and the Department of Homeland Securitys Security Science & Technology Directorate under Award Number DE-OE0000780.

Disclaimer

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

References

[1] Case, Defense Use. "Analysis of the cyberattack on the Ukrainian power grid." *Electricity Information Sharing and Analysis Center (E-ISAC)* (2016).

[2] Stouffer, Keith, Joe Falco, and Karen Scarfone. "Guide to industrial control systems (ICS) security." *NIST special publication* 800, no. 82 (2011): 16-16.

[3] US Department of Homeland Security. *Safeguarding and Securing Cyberspace*. https://www.dhs.gov/xlibrary/assets/pso-safeguarding-and-securing-cyberspace.pdf

[4] Rehak, David, Pavel Senovsky, Martin Hromada, and Tomas Lovecek. "Complex Approach to Assessing Resilience of Critical Infrastructure Elements." *International Journal of Critical Infrastructure Protection* (2019).

[5] Herrera, Luis-Carlos, and Olaf Maennel. "A Comprehensive Instrument for Identifying Critical Information Infrastructure Services." *International Journal of Critical Infrastructure Protection* (2019).

[6] Seppänen, Hannes, Pekka Luokkala, Zhe Zhang, Paulus Torkki, and Kirsi Virrantaus. "Critical infrastructure vulnerabilityA method for identifying the infrastructure service failure interdependencies." *International Journal of Critical Infrastructure Protection* 22 (2018): 25-38.

[7] Zobel, Christopher W. "Quantitatively representing nonlinear disaster recovery." *Decision Sciences* 45, no. 6 (2014): 1053-1082.

[8] Hwang, Ching-Lai, Young-Jou Lai, and Ting-Yun Liu. "A new approach for multiple objective decision making." *Computers & operations research* 20, no. 8 (1993): 889-899.

[9] Timashev, S. A. "Cyber Reliability, Resilience, and Safety of Physical Infrastructures." In *IOP Conference Series: Materials Science and Engineering*, vol. 481, no. 1, p. 012009. IOP Publishing, 2019.

[10] Kim, Anya, and Myong H. Kang. *Determining asset criticality for cyber defense*. No. NRL/MR/5540–11-9350. NAVAL RESEARCH LAB WASHINGTON DC, 2011.

[11] Ren, Jingzheng, and Benjamin K. Sovacool. "Quantifying, measuring, and strategizing energy security: Determining the most meaningful dimensions and metrics." *Energy* 76 (2014): 838-849.

[12] Shen, Lijuan, and Loon Ching Tang. "Enhancing resilience analysis of power systems using robust estimation." *Reliability Engineering & System Safety* 186 (2019): 134-142.

[13] Amin, S. Massoud. "Electricity infrastructure security: Toward reliable, resilient and secure cyber-physical power and energy systems." In *IEEE PES General Meeting*, pp. 1-5. IEEE, 2010.

[14] Haque, Md Ariful, Sachin Shetty, and Bheshaj Krishnappa. "Cyber-physical systems resilience: Frameworks, metrics, complexities, challenges and future directions". To appear in book of John Wiley and Sons, *Complexity Challenges in Cyber Physical Systems: Using Modeling and Simulation (M&S) to Support Intelligence, Adaptation and Autonomy*, 2019.

[15] Farzan, Farnaz, Mohsen A. Jafari, D. Wei, and Y. Lu. "Cyber-related risk assessment and critical asset identification in power grids." In *ISGT 2014*, pp. 1-5. IEEE, 2014.

[16] Gómez, Juan Fco, Pablo Martínez-Galán, Antonio J. Guillén, and Adolfo Crespo. "Risk-Based Criticality for Network Utilities Asset Management." *IEEE Transactions on Network and Service Management* (2019).

[17] Arghandeh, Reza, Alexandra Von Meier, Laura Mehrmanesh, and Lamine Mili. "On the definition of cyber-physical resilience in power systems." *Renewable and Sustainable Energy Reviews* 58 (2016): 1060-1069.

[18] Vugrin, Eric D., and R. Chris Camphouse. "Infrastructure resilience assessment through control design." *International journal of critical infrastructures 7*, no. 3 (2011): 243-260.

[19] Haque, Md Ariful, Gael Kamdem De Teyou, Sachin Shetty, and Bheshaj Krishnappa. "Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights." In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 25-30. IEEE, 2018.

[20] Mell, Peter, Karen Scarfone, and Sasha Romanosky. "A complete guide to the common vulnerability scoring system version 2.0." In *Published by FIRST-Forum of Incident Response and Security Teams*, vol. 1, p. 23. 2007.

[21] Haque, Md Ariful, Sachin Shetty, and Gael Kamdem. "Improving bulk power system resilience by ranking critical nodes in the vulnerability graph." In *Proceedings of the Annual Simulation Symposium*, p. 8. Society for Computer Simulation International, 2018.

[22] Haque, Md Ariful. "Analysis of Bulk Power System Resilience Using Vulnerability Graph." (2018). DOI: 10.25777/fqw2-xv37.

[23] Haque, Md Ariful, Sachin Shetty, and Bheshaj Krishnappa. "ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems." In *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing (HPSC), and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pp. 273-281. IEEE, 2019.

[24] Bharali, A., and Dimpee Baruah. "On network criticality in robustness analysis of a network structure." *Malaya Journal of Matematik (MJM)* 7, no. 2, 2019 (2019): 223-229.

[25] Roberson, Dakota, H. Clarisse Kim, Bo Chen, Christine Page, Reynaldo Nuqui, Alfonso Valdes, Richard Macwan, and Brian K. Johnson. "Improving Gird Resilience Using High-Voltage dc: Strengthening the Security of Power System Stability." *IEEE Power and Energy Magazine* 17, no. 3 (2019): 38-47.

[26] Tizghadam, Ali, and Alberto Leon-Garcia. "On robust traffic engineering in transport networks." In *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*, pp. 1-6. IEEE, 2008.

[27] Chung, Fan. "Laplacians and the Cheeger inequality for directed graphs." *Annals of Combinatorics* 9, no. 1 (2005): 1-19.

[28] Bernstein, Dennis S. *Scalar, Vector, and Matrix Mathematics: Theory, Facts, and Formulas-Revised and Expanded Edition*. Princeton university press, 2018.

[29] Saaty, Thomas L. "Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of intangible factors the analytic hierarchy/network process." *RACSAM-Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales. Serie A. Matematicas* 102, no. 2 (2008): 251-318.