IET Cyber-Physical Systems: Theory & Applications
Special section: Cyber-Physical Security Issues in Smart Grids

IET Journals
The Institution of Engineering and Technology

# ARCADES: Analysis of Risk from Cyber Attack against DEfensive Strategies for power grid

ISSN 1751-8644
doi: 0000000000
www.ietdl.org

*M. Touhiduzzaman*[1*], *A. Hahn*[1], *A. Srivastava*[1]

[1] *School of Electrical Engineering & Computer Science, Washington State University, Pullman, WA 99163, USA*
[*] *E-mail: md.touhiduzzaman@wsu.edu*

**Abstract:** In this paper, we introduce ARCADES, a technique to systematically explore the cybersecurity defense strategies based on contingency rankings in power systems. While cybersecurity defensive standards exist, these approaches are primarily based on expert opinions, rather than systematic studies of risk. ARCADES presents an approach to identify improved cybersecurity defensive strategies based on a graph-based cyber-physical security model that is evaluated by resistance-distance metrics and then prioritized based on contingency analysis studies of the system. This paper also proposed a technique that identifies the most critical cybersecurity mechanisms to protect the power grid. Planning and operation: those two applications for cyber security on power grid mainly explored in this paper. For planning, a systematic method is developed to verify the effectiveness of security strategies and for operation, prioritized the security mechanism for auditing and monitoring purpose. As a case study, we analyze the IEEE-14 bus, IEEE-30 bus and IEEE-118 bus system, observe the defensive strategies, and calculate substation criticality ranking by using our proposed method.

## 1 Introduction

Concerns for the cybersecurity of the grid have been continually raised by governments, utilities, public sector, and media. This risk was exemplified on December 23rd, 2015, when attackers were able to intrude into Ukraine distribution control centers and proceed to trip a large number of substation breakers, resulting in a substantial blackout [1].

Furthermore, it is well understood that many power grid security control system contain a number of vulnerabilities that remain undiscovered by utilities and vendors [2]. An increased presence of zero-day vulnerabilities further complicates risk assessment procedures as defenders possess incomplete information on threat system. Fortunately, the North American Electric Reliability Corporation (NERC) has introduced the Critical Infrastructure Protection (CIP) standards to ensure that the bulk power system is protected from such attacks. However, the scope of these requirements continues to evolve in an attempt to more accurately align the security controls with the risk from an attack. For example, in CIP Version 3, systems only required protection if they are identified as Critical Cyber Assets, which is on a variety of factors [3]. However, this approach leaves many systems unprotected and vulnerable to attack. More recently, NERC has introduced Version 5, which categorizes systems as low, medium, and high depending on their criticality, and requires different sets of security controls based on this criticality [28]. These controls are typically applied on perimeter devices through the context of an encapsulated security perimeter (ESP), which is used to prevent remote intrusions to sensitive internal systems. However, the adequacy, cost, and potential for interrupting key system operations provide continual debate over the defense strategies.

While the NERC-CIP standards ensure the U.S. grid maintains some level of protection, there are remaining questions of how to identify the set of security controls and system categorizations that most accurately reflect the grid's risk. An strategic placement of security controls is necessary to ensure the grid receives the greatest protection at the minimum cost to utilities as implementing and monitoring security controls frequently introduces a financial burden. The lack of strong and well accepted metrics is currently a key challenging to the area of cybersecurity [5]. In recent days, many new metrics have been proposed to access the security risk of traditional network [6] [7]. But improved cyber-physical security metrics are needed to help determine the most appropriate placement of security mechanisms to protect the grid.

In this paper, we present a novel technique to evaluate whether cyber defensive strategies and security mechanisms are adequately aligned with the risk of attack to different substations based on contingency analysis. Our main contribution of this work can be summarized as follows:

1. Introduce a graph-based security model, extending the work in [8] to model the difficulty of various attack paths and their potential to influence grid contingency scenarios (Section IV).
2. Propose a risk assessment methodology through the combination of a graph-based resistance-distance metric and impact factor contingency rankings to identify to provide cyber-physical risk indexes. (Section V)
3. Evaluate the proposed techniques on the IEEE 14-bus, IEEE-30 bus and IEEE-118 bus system and demonstrate (i) defensive strategies for substation protection, and (ii) identify improved allocations of security mechanisms to reduce overall system risks (Section VI).

## 2 Related Work

Multiple previous research efforts have attempted to quantify system security by analyzing the difficulty an attacker must exert to compromise that system. Early work in computer security introduced attack and privilege graphs, based on fault trees modules used to analyze system [9][10]. Work by [11] and [12] provides metrics based on path analysis in attack graphs, while additional metrics have been proposed to analyze attack surfaces[13]. More recent work has suggested a k-zero day safety metric to measure the number of zero day exploits that would be required to compromise system assets [14].

In [15], the authors applied attack trees to power systems to quantify the impact of the attack through the loss of load. Work by [16] has identified cyber-physical graph models to analyze attack impacts on power system dynamical models. Furthermore, work by [8] identified attack exposure metrics through the enumeration of attack paths to various objects within a power system Common Information Models (CIM). Work in [17] explores cyber-physical system awareness where attacks are modeled as time hidden Markov based

**Table 1** Key NERC Cybersecurity Requirements

| Standard | Requirement | Level |
|---|---|---|
| CIP-005-5 | R1.3: Enforce inbound and outbound access permissions | High, Medium |
| CIP-005-5 | R1.5: Mechanisms to detect malicious communication | High, Medium (control centers) |
| CIP-005-5 | R2.1: Remote interactive sessions direct to intermediate system | High, Medium (externally routable) |
| CIP-005-5 | R2.2: Encrypt remote interactive traffic to intermediate system | High, Medium (externally routable) |
| CIP-005-5 | R2.3: Multi-factor authentication for interactive sessions | High, Medium (externally routable) |
| CIP-003-7 | p.30: LERC implements network access control on addresses and ports | Low |

on attack graph models and analyzing data collected for both cyber and physical sensors. Work in [18] analyzes the reliability impact from successful cyber penetration in a substation that may result an unplanned breaker trip. By accessing the security mechanism of a SCADA system or substation through cyberattack can have serious impact [19] that can cause result of loadshedding, financial loss due to damage equipment or environmental damage.

Additional work has coupled cyber-based risk analysis and power system contingency analysis techniques to identify risks from cyber attack. In [20], the authors proposed a new metric named CPIndex based on incomplete information and cyber intrusion ranking methodology that calculate cyber-physical vulnerability assessment of smart grid. In [21], the authors introduced SOCCA to use information about the current security state of cyber system and physical system and rank contingencies induced by an attacker. In [22], the authors demonstrate novel techniques that model coordinate attacks to different power system components (e.g., power flow, generators, lines), which is important for analyzing comprehensive detection strategies that best protect from many potential attacks. Work in [23] proposed graph theory based centrality measure for vulnerability assessment of power grid that uses DC power flow based linear sensitivity factor. Unfortunately, there remain many challenges in accurately calculating cybersecurity metrics [24].

While numerous research efforts have proposed metrics to determine the security posture of various smart grid systems, none of these have introduced an approach to model the current defensive strategies (e.g., NERC CIP) currently being used to protect the power. In this paper, our proposed method systematically analyze defensive strategies used to protect the power grid.

## 3 Overview of Cyber Protection on Smart Grid

The NERC CIP standard is a common defensive strategy, where protection and detection techniques are defined proportionally to the potential negative impact of an attack to various cyber assets. Currently, NERC version 5 requires that systems be categorized as high, medium, or low based on their ability to impact the grid. High ratings are typically reserved to control centers overseeing significant generation (e.g.,3000 MW), otherwise they are categorized as medium. Substations are generally considered Low unless they support transmission facilities operated at 500 kV or higher, or operating between 200 kV and 499 kV at a single substation [28]. While the NERC security mechanisms include technical, managerial, and operational controls, this paper will focus on the technical controls. NERC standards that address prevention and detection include CIP-005-5 Electronic Security Perimeter (ESP) [28], CIP-007-5 System Security Management [29], and CIP-003-7 Security Management Controls [30].

Both high and medium criticality assets require an ESP to provide isolation between untrusted networks and critical substations and control centers, while CIP Version 5 introduces a requirement for Low ESPs for all other assets. The ESP is protected by an electronic access point (EAP) which implements a variety of critical protection mechanisms to prevent malicious communication from entering the ESP through remote interactive sessions that primarily include human access (e.g., maintenance, engineering) and also this EAP allows routable communication between cyber assets.

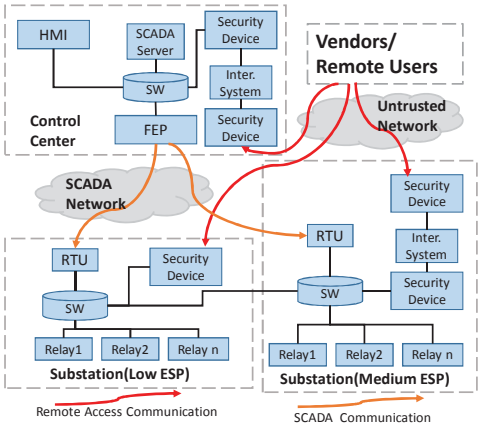



**Fig. 1**: Example ESP Architecture

Table I provides an overview of the key security standards required by NERC. the technical protection or detection mechanism, and the level of the control (e.g., high, medium, low) The NERC ESP standards introduced by CIP-005-5 requires that medium and high ESPs implement network access control on both incoming and outgoing traffic to prevent malicious traffic and mechanisms to monitor malicious communications. CIP-005-5 also provides additional security requirements to protect remote interactive sessions, including communication encryption and multi-factor authentication. There are requirements for redundant security devices in ESPs to reduce the probability that a single vulnerability will provide access to the substation. Figure 1 provides an overview of the required protection strategies in both ESP and LESP, demonstrating the security mechanisms the protect both interactive and SCADA communication sessions. In this paper, we have considered a substation either High Impact Substation (*HIS*) and Low Impact Substation (*LIS*). We assumed those *HIS* and *LIS* required protection strategies same as ESP and LESP, respectively.

## 4 Modeling Security Graph for Risk Assessment Approach

The smart grid expands the capabilities of the traditional electric power grid by introducing some new characteristics such as two-way communication, substation automation, deployment of distributed energy resources, self-healing, wide area measurement system, energy storage system, SCADA, smart metering, etc. The domain of attack surface of the smart grid for cyberattack have been increased due to more substantial information and communication technology (ICT) dependencies [25]. In this section, we are focusing on the defensive strategies of electronic security perimeter(ESP) related to SCADA and substation automation by developing security graph model.

Graph-based modeling and resistance distance metrics will be used to evaluate the effectiveness of the defensive strategy, while power flow analysis and impact factor calculation used to determine the power system impacts as demonstrated in Figure 2. In our proposed technique, two metrics have been incorporated to calculate the cyber-physical risk assessment that comprehensively model and analyze the level of protection. Figure 2 also shows the flowchart of our proposed technique to find the criticality of the substation.

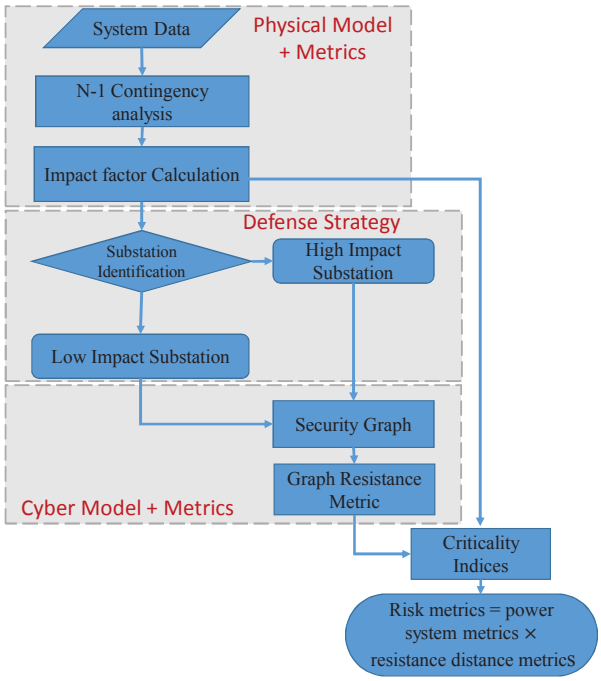



**Fig. 2**: Impact Assessment Approach

### 4.1 Physical System Model

We assume an intruder attempt to seek strategies to find out the most critical substations and tries to manipulate those substations control parameter to cause damage as much as possible. Hence from power utility perspective, the most critical substation need to be identified and equipped with well protection devices to protect from cyber-attack. In our physical system model, we have assumed that each is equipped with protection devices such as IP-based IED, VPN, Firewall, etc. According to the NERC guideline criteria, all kind of substations (generation, transmission & distribution) in bulk power system are identified as potential critical assets [31].

In our physical system model, we have used two strategies to find the substation criticality: first, $N-1$ contingency analysis and then impact factor calculation. Based on these two strategies, we have categorized *HIS* and *LIS*.

In $N-1$ contingency analysis, '$-1$' refer to the failure of a single element of a substation or multiple elements that are physically and electrically connected to each other failed together as a one [32]. Single contingencies are considered critical because multiple element failures in a substation due to cyber-attack is plausible even though this type failure is less likely than single element failure. In our first strategy, we remove a substation under normal operating condition. If the removal of a substation under normal operating condition results in non-convergent power flow solution, then this substation is considered as the most critical substation. This substation needs careful attention with advanced cybersecurity protection by treating as *HIS*.

The author in [33] introduced the impact factor metrics, $\gamma$ which represent the impact of removal a substation from the entire power system. This impact factor calculation is applicable for the analysis of cyber attack in power system.The impact factor is defined as follows:

$$\gamma = \left(\frac{P_{lol}}{P_{total}}\right)^{L^*-1} \quad (1)$$

In this equation, $L^*$ represent the value of loading level, $L$ where power flow diverges. This loading level, $L$ is achieved by continuation power flow method, i.e. P-V curve analysis. Here $P_{lol}$ and $P_{total}$ represent the loss of load and total system load respectively. In this method, substations are designated as the highest level of criticality whose impact factor, $\gamma = 1$. In this paper, our strategy is to calculate the impact factor of the entire power system by not including *HIS* those are found during $N-1$ contingency analysis. Then, the impact factor of each substation is ranked in descending order to determine the most critical substation. Based on this rank, we choose few substations as *HIS* and others as *LIS*.

The 'Gordon-Loeb' model [34] [35] determines the impact factor threshold to categorize each substation. This model helps to determine the optimum level investment of cyber asset based on the asset economic impact when this asset is compromised. This model expands analysis in critical infrastructure industry too. For this paper, our cost of a cyber security breach incorporates to loss of load ($P_{lol}$). In practice, when making the security investment decision, the utility should choose an impact factor threshold in such a way that total loss of load is minimized.

According to this model, it was found that a system planner will not invest more that 37% of the expected loss from the overall security breach. To obtain the impact factor threshold value, we list all the substations in descending order according to the impact factor. Then we sum the loss of load values, progressively until it reaches 37% of the total expected loss. When the criteria is met, that substation impact factor is considered as threshold value. This allows us to define the substation security investment based on potential losses. Figure 3 shows the substation categorization algorithm.

```
1:  Input: List of substation data
2:  Output: HIS, LIS
3:  for all s_i sϵ substations
4:          Remove s_i and run NR power flow
5:          if (network converges) then
6:              Add s_i to temp
7:          else
8:              Add s_i to HIS
9:  End for
10: for all  s_i in temp
11:         Determine Impact factor (γ) of s_i
12:         if (γ ≥ threshold) then
13:             Add s_i to HIS
14:         else
15:             Add s_i to LIS
16: End for
```

**Fig. 3**: Substation Categorization Algorithm

The objective of the attacker is to manipulate the protection devices(e.g. relays, IP-based IED) which will create impact on the power system reliability and security. These protection devices provide all required view for monitoring, operation, protection, etc. In this paper, attacker exploits the vulnerabilities of protection devices which eventually bring down the substation.

### 4.2 Cyber Model

A graph-based model, $G = (C, L)$ is used for the cyber system to include the set of cyber assets, $C$, and network links $L$ connecting them. A set of links is grouped into a network, $K$, if all systems are reachable across this set of links. Furthermore, $D$ represents the set of data transmitted across the system, which includes the operational information standardized by modern common information models (e.g., IEC 61970, IEC 61968) [36].

This basic cyber model needs to be expanded to include security properties that help analyze the controls used to protect the substations. We define a set of security controls $S$ (e.g., access control, authentication, firewalls) used to protect various system privileges that provide access to some data $D$ used in protection devices and also connected networks $K$. Furthermore, the mapping $sec \subseteq S \times P$ identifies the security mechanisms used to protect each privilege. We assume that an external attack begins with the empty privilege set $P_A = \langle \emptyset, K_0 \rangle$, where $K_0$ represents an external untrusted network.

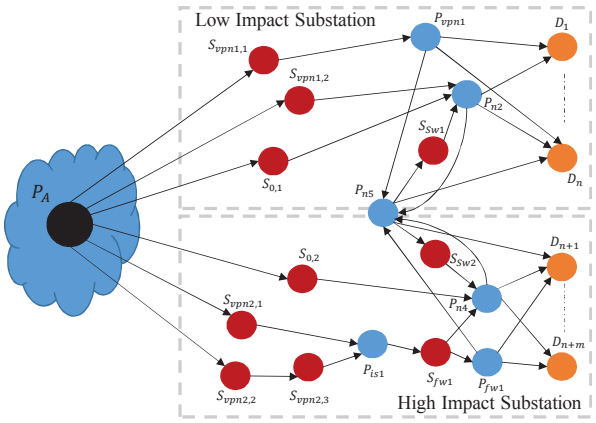



**Fig. 4**: An proposed security graph model where exists one HIS and one LIS. This security graph model considers all possible paths that an attacker could traverse to gain substation common data (orange) by manupulating security mechanisms (red) and privilegdes (blue)

The previously defined model will be converted to a security graph which is used to model all possible paths that an attack could traverse to manipulate some data across its path from the sender to receiver. The directed security graph is defined as $G_s = (P \cup S \cup D, E)$, where $E$ is defined as:

$$E = \begin{cases} \{p, s\}, w = w_s & \exists n \exists c | s \in c \wedge n \in p \wedge c \in n \\ \{s, p\}, w = 0 & \forall \{s, p\} | \{s, p\} \in sec(.) \\ \{p, p'\}, w = 0 & \forall p' \in p \\ \{p, d\}, w = 0 & \forall d \in p \end{cases} \quad (2)$$

Based on this proposed model, a security graph will be created based on the NERC CIP cybersecurity technical requirements. Individual weights, $w_s$, can be added based on the effectiveness of the security mechanisms. This will be used to analyze the security of various substations. This section will only demonstrate the security graph for both *HIS* and *LIS*. This model makes the following assumptions: (i) some network access control mechanisms is used to protect SCADA communication, and (ii) that substations are interconnected across lines in order to support transfer trip relay messages between connected substations, and (iii) that substation switches use access control lists (ACLs) to ensure a relay in one substation can only connect a single relay in another substation, and (iv) multiple security mechanism used in a single device, and (v) that other substation devices (e.g., RTUs) do not implement any security controls. Figure 4 demonstrates the proposed security graph based on the system model defined in Table II.

## 5 Attack Analysis Metrics

This section will introduce a cyber-physical techniques to measure the grids risk to cyber attack based on the proposed security graph and contingency rankings. Graph resistance method has been applied to analyze the previously proposed algorithms to quantify the system vulnerability [38]. As identified in [11], attack difficulty is based on the length and quantity of paths between attackers and defenders. In this section, first we discuss about the properties of resistance distance by giving an example. Next, we developed criticality indices by corelating with resistance distance metrics to identify which power system components are most vulnerable to cyber attacks.

### 5.1 Resistance Distance

Klein and Randic [39] first introduced resistance distance to quantify number of important properties of graph network. In our paper, we utilize the resistance distance metric, which conceptualizes the electric resistance in a graph where each edge represents the ohms. Each of the vertices in the graph satisfies Kirchhoffs law of current

**Table 2** Example Security Model

| | |
|---|---|
| Cyber Model($C$) | $(N_0, c_{vpn1}), (c_{vpn1}, c_{sw1}), (c_{fep}, c_{rtu1})$ $(c_{rtu1}, c_{sw1}), (c_{sw1}, c_{relay1}), (c_{sw1}, c_{relay2})$ $(N_0, c_{vpn2}), (c_{vpn2}, c_{is1}), (c_{fep}, c_{rtu2})$ $(c_{is1}, c_{fw1}), (c_{fw1}, c_{sw2}), (c_{rtu2}, c_{sw2}),$ $(c_{sw2}, c_{relay3}), (c_{sw2}, c_{relay4})$ |
| Networks ($K$) | $n_0 = \{*, c_{vpn1}, c_{vpn2}\}$ $n_1 = \{c_{fep}, c_{rtu1}, c_{rtu2}\}$ $n_2 = \{c_{vpn1}, c_{sw1}, c_{rtu1}, c_{relay1}, c_{relay2}\}$ $n_3 = \{c_{vpn2}, c_{is1}, c_{fw1}\}$ $n_4 = \{c_{fw1}, c_{sw2}, c_{rtu2}, c_{relay3}, c_{relay4}\}$ $n_5 = \{c_{relay2}, c_{sw1}, c_{sw2}, c_{relay3}\},$ |
| Protection Devices ($D$) | $cb_op_1, cb_op_2, cb_op_3, cb_op_4$ |
| Privileges ($P$) | $p_A = \langle\{\emptyset, \emptyset\}\rangle$ $p_{vpn1} = \langle\{cb_op_1, cb_op_2\}, \emptyset\}\rangle$ $p_{fw1} = \langle\{cb_op_3, cb_op_4\}, \emptyset\}\rangle$ $p_{n2} = \langle\{cb_op_1, cb_op_2\}, p_{n5}\}\rangle$ $p_{n4} = \langle\{cb_op_3, cb_op_4\}, p_{n5}\}\rangle$ $p_{n5} = \langle\{cb_op_2, cb_op_3\}, \emptyset\}\rangle$ $p_{is1} = \langle\{cb_op_3, cb_op_4\}, \emptyset\}\rangle$ |
| Security Mechanisms ($S$) | $s_{0,1}$ = Network Access Control (SCADA) $s_{0,2}$ = Network Access Control (SCADA) $s_{vpn1,1}$ = System Access Control $s_{vpn1,2}$ = System Authentication (Int) $s_{vpn2,1}$ = System Access Control $s_{vpn2,2}$ = System Auth. (Factor 1) $s_{vpn2,3}$ = System Auth. (Factor 2) $s_{fw1}$ = System Access Control $s_{sw1}$ = Network Access Control $s_{sw2}$ = Network Access Control |
| Privilege Mappings ($sec()$) | $\{s_{vpn1,1}, p_{vpn1}\}, \{s_{vpn1,2}, p_{n2}\},$ $\{s_{0,1}, p_{n2}\}, \{s_{sw1}, p_{n2}\}, \{s_{0,2}, p_{n4}\},$ $\{s_{vpn2,1}, p_{is1}\}, \{s_{vpn2,2}, s_{vpn2,3}\},$ $\{s_{vpn2,3}, p_{is1}\}), \{s_{fw1}, p_{is1}\},$ $\{s_{sw2}, p_{n4}\}$ |

conservation. Consider a graph network where the potential of each vertices $i$ is $v_i^{(s,t)}$. This potential is measured by treating source $s$ and target $t$ potential as a reference. According to Kirchhoffs law each of vertices satisfies following equation:

$$\sum_j A_{i,j}(v_i^{(s,t)} - v_j^{(s,t)}) = u_i^{(s,t)} \quad (3)$$

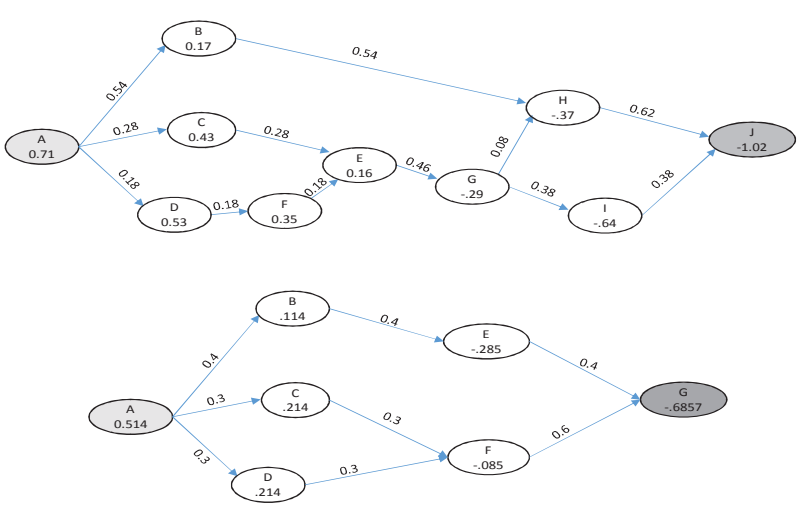
Here, $A$ is the adjacency matrix and u is the supply outlet where current enter and leave the network. This eqaution shows how much current flow through edge $(i, j)$. This Eq.(3) can be written as graph-laplacian matrix form:

$$(D - A)v^{(s,t)} = Lv^{(s,t)} = u^{(s,t)} \quad (4)$$

Where, $D$ is the degree(the number of edges incident) of a vertex and $L = D - A$ is the graph-laplacian matrix. Then, the Moore-Penrose generalized inverse graph laplacian matrix is $L^+$ and the solution of Eq.(4) become:

$$v_i^{(s,t)} = L^+ u^{(s,t)} = L^+_{i,s} - L^+_{i,t} \quad (5)$$

This generalized inverse graph laplacian matrix, $L^+$ compute vertices potential for any source-target vertices. To calculate resistance




| | A | B | C | D | E | F | G | H | I | J |
|---|---|---|---|---|---|---|---|---|---|---|
| A | 0.55 | 0.20 | 0.26 | 0.29 | 0.06 | 0.13 | -0.09 | -0.05 | -0.17 | -0.16 |
| B | 0.20 | 0.65 | 0.03 | 0.02 | -0.04 | -0.06 | 0.01 | 0.20 | -0.03 | 0.03 |
| C | 0.26 | 0.03 | 0.69 | 0.15 | 0.23 | 0.14 | -0.04 | -0.10 | -0.16 | -0.18 |
| D | 0.29 | 0.02 | 0.15 | 0.79 | 0.11 | 0.40 | -0.13 | -0.15 | -0.23 | -0.24 |
| E | 0.06 | -0.04 | 0.23 | 0.11 | 0.49 | 0.25 | 0.10 | -0.05 | -0.05 | -0.10 |
| F | 0.13 | -0.06 | 0.14 | 0.40 | 0.25 | 0.77 | -0.06 | -0.15 | -0.19 | -0.22 |
| G | -0.09 | 0.01 | -0.04 | -0.13 | 0.10 | -0.06 | 0.50 | 0.20 | 0.30 | 0.20 |
| H | -0.05 | 0.20 | -0.10 | -0.15 | -0.05 | -0.15 | 0.20 | 0.54 | 0.22 | 0.33 |
| I | -0.17 | -0.03 | -0.16 | -0.23 | -0.05 | -0.19 | 0.30 | 0.22 | 0.84 | 0.48 |
| J | -0.16 | 0.03 | -0.18 | -0.24 | -0.10 | -0.22 | 0.20 | 0.33 | 0.48 | 0.86 |

| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| A | 0.465 | 0.151 | 0.194 | 0.194 | -0.020 | 0.065 | -0.049 |
| B | 0.151 | 0.637 | -0.020 | -0.020 | 0.265 | -0.049 | 0.037 |
| C | 0.194 | -0.020 | 0.622 | 0.122 | -0.092 | 0.194 | -0.020 |
| D | 0.194 | -0.020 | 0.122 | 0.622 | -0.092 | 0.194 | -0.020 |
| E | -0.020 | 0.265 | -0.092 | -0.092 | 0.694 | -0.020 | 0.265 |
| F | 0.065 | -0.049 | 0.194 | 0.194 | -0.020 | 0.465 | 0.151 |
| G | -0.049 | 0.037 | -0.020 | -0.020 | 0.265 | 0.151 | 0.637 |

**Fig. 5**: Comparison of two resistor network with respect to resistance distance where all resistance are equal to unity. Each of the vertex is labled with letter and its potential when a unit current is injected from A and entering to J(figure above) and G(figure below). Each of the edge is leveled with current flowing. The Moore-Penrose generalized inverse graph laplacian matrix,$L^+$ of each netwok also shown in the figure.

distance, we need to consider the graph network as a resistor network. The resistance distance $r_{i,j}$ is the effective resistance between vertices $i$ and $j$ which represents as the potential difference between vertices $i$ and $j$ when a unit current is leaving from vertex $i$ and entering vertex $j$:

$$r_{i,j} = v_i^{(i,j)} - v_j^{(i,j)}$$

$$r_{i,j} = (L^+)_{ii} + (L^+)_{jj} - (L^+)_{ij} - (L^+)_{ji} \tag{6}$$

An simple example of two resistor network is shown in Fig.(5) where figure above and figure below network is similar to HIS and LIS, respectively. Here, all the vertices satisfies Kirchhoffs law. Also, the current leaving from source vetex A is 1 and enter the target vertex J(figure above) and G(figure below) is 1. The effective resistance (distance) from source to target is 1.73 (figure above) and 1.1997 (figure below). From this effective resistance, we can conclude that it will required more effort for source A to reach target J rather than target G.

The resistance distance shows the following properties: path redundancy, path length, multiple path, etc. Those properties are well aligned to the characteristics of graph such as closeness centrality, betweenness centrality, etc. Previously, a very few works considered closeness centrality and betweenness centrality to find the criticality of the substation [20] [37]. In this paper, resistance distance is used as an index of node vulnerability to quantify an attack difficulty to travel various paths where a larger resistance distance is less vulnerable due to increased effort required for the attacker to traverse the security mechanisms [38]. Also, resistance distance acts as a key performance measure to study the robustness of a graph network when we have security mechanism insertion and/or removal. The result of the resistance distance metrics will be developed to identify which power system components are most vulnerable to cyber-attacks.

### 5.2 Substation Criticality Ranking

For the security graph, $G_s$, the graph Laplacian matrix $L^s$ is defined as:

$$L^s = D^s - A^s$$

where, $A^s$ is the adjacency matrix and $D^s$ is the degree matrix of the security graph. Resistance distance, $r^s$ is computing by creating the pseudo-inverse $(L^+)^s$ of the graph Laplacian matrix of security graph, $L^s$.

$$r_{ij}^s = (L^+)_{ii}^s + (L^+)_{jj}^s - (L^+)_{ij}^s - (L^+)_{ji}^s \tag{7}$$

The overall network criticality in term of the undirected Moore-Penrose Laplacian matrix can be analyzed using normalized total resistance distance that represents as follows:

$$\vec{r} = \frac{1}{n(n-1)} \sum r_{ij}^s = \frac{2}{n-1} Tr(L^+)^s \tag{8}$$

Here, $n$ is the number of nodes. Let, $\eta_i$ is the criticality of node $k$ which is described as an average distance of a node from its neighbours. This node criticality is defined as:

$$\eta_i = \frac{n(n-1)}{2} \vec{r} = \frac{1}{n} \sum_j r_{ij}^s \tag{9}$$

A resistance distance metrics associated with security mechanisms and privileges is:

$$\mathbf{r_{ai}^s} \in r^{n \times n}, \quad n = |C|$$

In this matrix, $r_{ai}^s$ defined as the resistance distance from attacker node $a$ to protection device $d$ of any substation $i$. The criticality of the substation under cyberattack, $\Gamma$ is the product of the impact factor index and resistance distance metrics which measure how much vulnerable of a substation regarding to an certain attack path. The substation criticality index is based on attack path vulnerability of that specific substation which is describe as follows:

$$\Gamma_i = \gamma_i \times r_{ai}^s \tag{10}$$

where, $\gamma_i$ is the impact factor index of substation $i$. Substation criticality ranking have been found by arranging $\Gamma$ of all substation in descending order.

### 5.3 Cybersecurity Control Ranking

In our proposed cyber-physical model, we have allocated the cyber security control within the substation ESP by considering the cyber defense strategies. Deployment of the security controls provide more efficient control, reliability, flexibility and attack prevention technique compared to traditional power network. For example, multi factor authentication added one more security layer at a low cost which reduce the risk of a cyber-attack [40]. Although, they provide some defense, they might contain software vulnerabilities which can lead to a cyber-attack. When calculating the criticality of the cybersecurity control, our proposed risk assessment model considered all possible attack paths and assume an adversary is capable to exploit

the vulnerabilities by directing cyberattacks such as data integrity attack, data spoofing, replay attack, etc.

The criticality of a cybersecurity control protections is based on the importance of its ability to restrict information or access flows from attackers to various data or systems. we assume that the attacker compromised the security mechanism of substation $i$. A resistance distance matrix without that compromised security mechanism is calculated as follows:

$$\mathbf{r}^{s}_{\mathbf{aics}} \in r^{m\times m}, \quad m = n-1 = |C|-1$$

From this matrix, we obtain $r^{s}_{aics}$ which is the resistance distance matrix from attacker node $a$ to protection device $d$ of any substation $i$ without that compromised security mechanism located between the protection device $d$ of substation $i$ and attacker node $a$. The difference of resistance distance between $r^{s}_{aics}$ and $r^{s}_{ai}$ is multiplied with the impact factor index to find the criticality of that compromised security mechanism located in substation $i$. The criticality of cybersecurity control, $\alpha$ can be represent as follows:

$$\alpha_i = (r^{s}_{aics} - r^{s}_{ai}) \times \gamma_i \tag{11}$$

To find the criticality ranking of cybersecurity control, we arranged the criticality of cybersecurity control, $\alpha$ of all components in descending order. It is noteworthy to mention that as the electric power system become larger, there is less probability of cascading failure due to $N-1$ contingency [32] and the criticality of a single asset become even smaller. The higher this $\alpha$ is, the worse the risk of not meeting the system operation and planning criteria. The normalization in (8) put $\alpha$ in to the same level ((0,1) range) which improve indices integrity and makes it convenient for the further criticality analysis. This normalization also gives the assurance of accuracy and consistency of criticality indices over different electric power system.

$$\alpha_{[0,1]} = (\alpha_i - \alpha_{min})/(\alpha_{max} - \alpha_{min}) \tag{12}$$

In this paper, we used multiple power systems that vary in size to helps us to quantify the computational complexity of our proposed substation and cybersecurity ranking method. We used the time taken to run our algorithm on different network sizes to experimentally determine our model complexity. As our indices iterating over linear equation, the computational complexity of our method become $\mathcal{O}(n^2)$ , where n is the number of nodes in the system.

## 6 Case Study

The proposed methodology is implemented in IEEE-14 bus, IEEE-30 bus and IEEE-118 bus system [41] to explore the criticality of the substations and the cybersecurity controls that protect the substation. Although, we had done the simulation of IEEE-118 bus system, but in this paper, we mostly focus on the result analysis of IEEE-14 bus and IEEE-30 bus system. We have used MATLAB and Python to implement and analyze our proposed algorithms.

### *6.1 Analysis of Physical System*

First, we have identified the most critical substation from the entire power system. To do this, we had removed a substation under normal operating condition and this $N-1$ contingency is done by removing all the transmission line or generator or load connected to that substation. Then Newton Raphson load flow is performed for this single outage. We have found that substation 2 of IEEE-14 bus and IEEE-30 bus system; and substation 68 of IEEE-118 bus system are the most critical substations . Those most critical substations need careful attention by treating as *HIS*.

According to section $IV.A$, the remaining substations other than the most critical are subject to impact factor analysis by using equation $(1)$. Table III and IV shows the substation categorization based on impact factor for IEEE-14 bus and IEEE-30 bus system, respectively. In those table, column 2, 3 and 4 represents the associated bus of each substation, expected loss of load due to cyber attack and maximum loadibility respectively. The impact factor threshold(bold value) that catagorized the substations is also shown in the table. The list of *HIS* for IEEE-14 bus, IEEE-30 bus and IEEE-118 bus system are:

**Table 3** Substation categorization for IEEE 14-bus system

| Sub. | Associated Bus | LOL(MW) | $L^*$ | $\gamma$ | Substation Categorization |
|---|---|---|---|---|---|
| 1 | 1 | 0.5 | 3.00 | 0.000071 | LIS |
| 2 | 2 | 5 | 1.00 | 1.0 | HIS |
| 3 | 3 | 94.24 | 3.059 | **0.2427** | HIS |
| 4 | 4,7,8,9 | 29.50 | 1 | 1.0 | HIS |
| 5 | 5,6 | 11.20 | 1.8 | 0.1050 | LIS |
| 6 | 10 | 9.00 | 3.066 | 0.0019 | LIS |
| 7 | 11 | 3.5 | 3.062 | 0.00027 | LIS |
| 8 | 12 | 6.1 | 3.04 | 0.00092 | LIS |
| 9 | 13 | 13.5 | 3.059 | 0.0044 | LIS |
| 10 | 14 | 14.9 | 3.066 | 0.0053 | LIS |

**Table 4** Substation categorization for IEEE 30-bus system

| Sub. | Associated Bus | LOL(MW) | $L^*$ | $\gamma$ | Substation Categorization |
|---|---|---|---|---|---|
| 1 | 1 | 0.3 | 2.5 | 0.00062 | LIS |
| 2 | 2 | 21.7 | 1.8 | 0.1766 | HIS |
| 3 | 3 | 2.4 | 2.5 | 0.0014 | LIS |
| 4 | 4,12,13 | 18.8 | 1.4 | 0.3968 | HIS |
| 5 | 5 | 0.0 | 2.5 | 0.0 | LIS |
| 6 | 6,9,10,11 | 5.8 | 1 | 1.0 | HIS |
| 7 | 7 | 22.8 | 2.8 | 0.0221 | HIS |
| 8 | 8 | 30 | 3.6 | **0.0083** | HIS |
| 9 | 14 | 6.2 | 2.9 | 0.0015 | LIS |
| 10 | 15 | 8.2 | 3 | 0.0019 | LIS |
| 11 | 16 | 3.5 | 2.6 | 0.0017 | LIS |
| 12 | 17 | 9 | 2.9 | 0.0031 | LIS |
| 13 | 18 | 3.2 | 3.1 | 0.00018 | LIS |
| 14 | 19 | 9.5 | 2.9 | 0.0034 | LIS |
| 15 | 20 | 2.2 | 2.9 | 0.000189 | LIS |
| 16 | 21 | 17.5 | 2.6 | 0.0021 | LIS |
| 17 | 22 | 0.0 | 2.2 | 0.0 | LIS |
| 18 | 23 | 3.2 | 2.7 | 0.00097 | LIS |
| 19 | 24 | 8.7 | 2.9 | 0.0029 | LIS |
| 20 | 25 | 0.0 | 2.8 | 0.0 | LIS |
| 21 | 26 | 3.5 | 2.8 | 0.00075 | LIS |
| 22 | 27,28 | 0.0 | 1 | 1 | HIS |
| 23 | 29 | 2.4 | 2.8 | 0.000384 | LIS |
| 24 | 30 | 10.6 | 2.8 | 0.0056 | LIS |

$$Subs_{14bus} = (2, 3, 4)$$

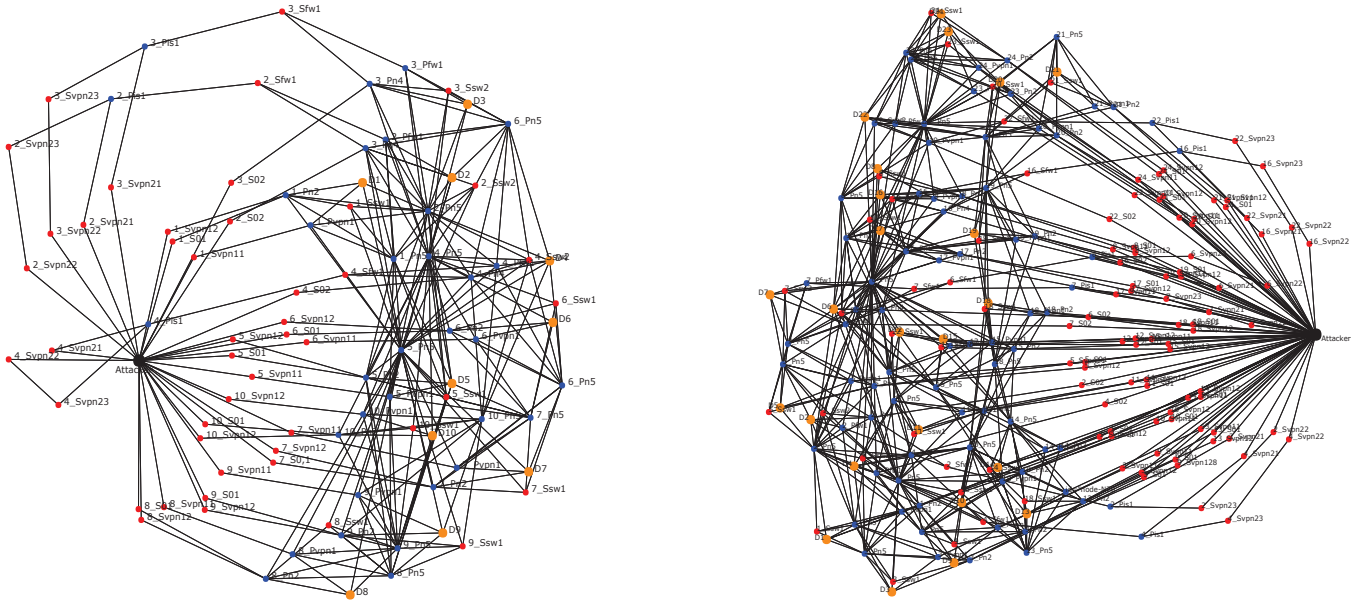
$$Subs_{30bus} = (2, 4, 6, 7, 8, 22)$$

$$Subs_{118bus} = (11, 15, 27, 42, 49, 54, 59, 60, 62, 68, 78, 80, 110, 116)$$

We allocated those substations according to 'Gordon-Loeb' model which shows that it is uneconomical to invest more than 37 percent of expected loss of load from the occur by entire security breach.

### *6.2 Development of Security Graph*

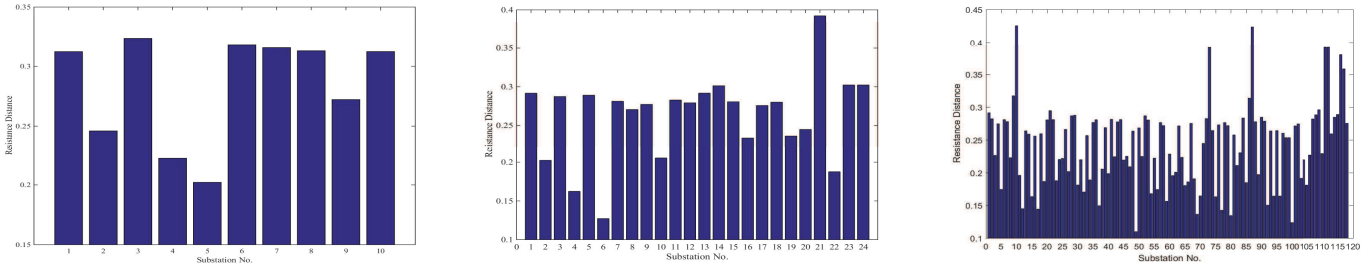
Our next goal is to develop a security graph corresponding to the IEEE bus system. The security graph for IEEE-14 bus and IEEE-30 bus system are shown in Figure 6.a and Figure 6.b, respectively. In our security graph red, blue, orange and black circle represents




(a) IEEE-14 bus system

(b) IEEE-30 bus system

**Fig. 6**: The security graph of IEEE-14 bus (Fig.6.a) and IEEE-30 bus (Fig. 6(b)) system. These security graph is modeled based on Table 2 where we assumed each substation contain one common data (protection device, $D$). In IEEE-14 bus(Fig. 6.a)) system, there are total 3(three) HIS and 162 attacking paths; and IEEE-30 bus (Fig.6.b) system, there are total 6(six) HIS and 288 attacking paths to reach the substation common data.




(a) IEEE-14 bus system

(b) IEEE-30 bus system

(c) IEEE-118 bus system

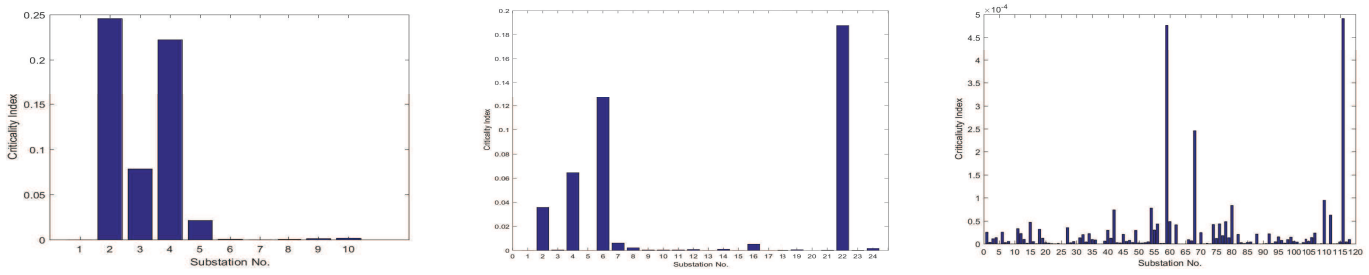
**Fig. 7**: Resistance distance from attacker to substation common data for IEEE-14 bus system(Fig. 7.a), IEEE-30 bus (Fig. 7.b) and IEEE-118 bus(Fig. 7.c) system. The attacking path to reach the substation 2, 3, 4 in IEEE-14 bus system(Fig. 7.a) ; substation 2, 4, 6, 10, 22 in IEEE-30 bus system (Fig. 7.b) and substation 12, 17, 38, 49, 68, 102 in IEEE-118 bus system(Fig.7.c) are more vulnerable, as their resistance distances are lower than others.

security mechanism, security privilege, substation protection device, and the attacker, respectively. This security graph is developed based on Table 2.

### *6.3 Cybersecurity Analysis of Security Graph*

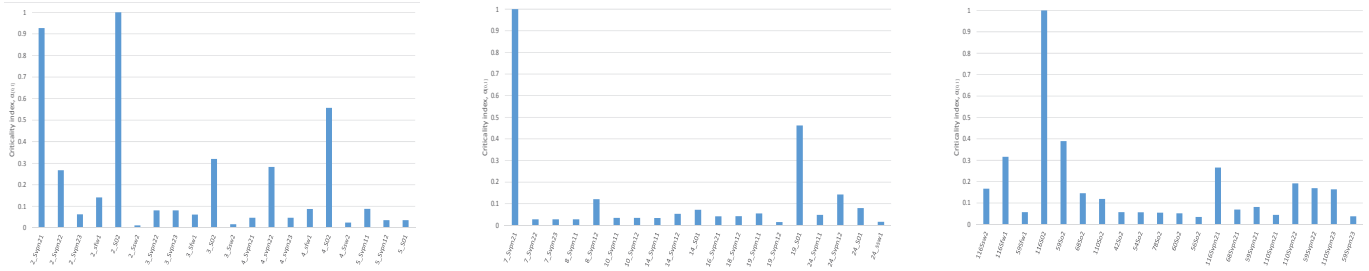
*6.3.1 Substation criticality ranking:* We have calculated the graph resistance distance for IEEE-14 bus , IEEE-30 bus and IEEE-118 bus system based on Eq. (7). The graph resistance distance matrices are obtained from security graph. Figure 7 shows the graph resistance distance from attacker to protection device for different substation of IEEE bus system. We have observed that resistance distance from attacker to protection device of substation 2, 4 and 5 for IEEE-14 bus system (Fig.7.a); substation 2, 4, 16, and 22 for IEEE-30 bus system (Fig.7.b); and substation 12, 17, 38, 49, 68 and 102 for IEEE-118 bus system (Fig.7.c) are lower than remaining substation. According to resistance distance metrics, lower resistance distance indicate that the specified attacking path is more vulnerable than others. Eq. (10) is used to calculate $\Gamma$ which represent the criticality of the substation under cyberattack. Figure 8 shows the substation criticality index under cyberattack for IEEE-14 bus(Fig.8.a), IEEE-30 bus (Fig.8.b) and IEEE-118 bus (Fig.8.c) system. This substation criticality indices based on resistance distance for cyber-physical system gives a new set of criticality ranking which is slightly different than physical system ranking. Substation 5 of IEEE-14 bus system; substation 8, 24 of IEEE-30 bus system and substation 112 of IEEE-118 bus system considered as critical even though these substations are considers as *LIS* in physical system ranking.

*6.3.2 Cybersecurity control ranking:* We calculate the criticality of each substation security mechanism as defined in Section 5.3. The criticality of each mechanism, $\alpha$ is calculated by using Eq. (11) and normalized within range $[0, 1]$ using Eq.(12). Figure. 9.a, 9.b and 9.c shows the first 20 (twenty) high critical($\alpha_{[0,1]}$) security mechanism located on IEEE-14 bus, IEEE-30 bus and IEEE-118 bus system, respectively. From Fig.9.a, network access control, $S_{0,2}$ and system access control, $S_{vpn2,1}$ of substation 2 ; from Fig. 9.b, system access control, $S_{vpn2,1}$ of substation 7 and network access control, $S_{0,1}$ of substation 19; and from Fig.9.c, network access control of substation 116 and 59 identified as the most critical security mechanisms among all the security mechanism located in IEEE-14 bus, IEEE-30 bus and IEEE-118 bus system, respectively. From this figure, we can conclude that most of the critical security mechanism located on the *HIS*. Also, very few *LIS* network access control shows high criticality because of their associative connectivity to *HIS*.




(a) IEEE-14 bus system (b) IEEE-30 bus system (c) IEEE-118 bus system

**Fig. 8**: Substation criticality ranking of different IEEE bus system. From the figure, it was observed that as the power system become larger, the substation criticality indices become smaller. The main reason is that larger systems have a better chance of surviving cascading failures due to an $N-1$ cyber contingency.



(a) IEEE-14 bus system (b) IEEE-30 bus system (c) IEEE-118 bus system

**Fig. 9**: First 20 high critical ($\alpha$) cybersecurity control for different IEEE bus system. This figure shows the normalize value(0,1) of cybersecurity control indices. It was observed that most of the high critical cybersecurity control are located in HIS due to its associative connectivity and contingency selection.

#### *6.3.3 Prioritization of placement in security mechanism:*

In this paper, we also observe what is the criticality of a substation after changing the security mechanism. This change of security mechanism gave us a clear perception about the criticality of a substation. For example, if we add more security mechanism in the most critical substation, the criticality of that substation will decrease. In our test case system, first we remove the three least critical security mechanism-i.e., all those are network access control, $s_{sw1}$ of *LIS* and then this removed security mechanism is placed between the privileges, $p_{n5}$ and network access control,$s_{sw2}$ on the three most critical substation. Table V shows the new ranking of three most critical substation after adding the security mechanism. From this table, we observed that most of the critical substation become less critical as we added new security mechanism to that substation.

**Table 5** Effect of change of security mechanism

| Test case | Sub. No | Graph based contingency ranking | Ranking after change the security mechanism |
|---|---|---|---|
| IEEE-14 | 2 | 1 | 3 |
| | 4 | 2 | 6 |
| | 3 | 3 | 7 |
| IEEE-30 | 22 | 1 | 4 |
| | 6 | 2 | 7 |
| | 4 | 3 | 9 |

### *6.4 Discussion*

The models and analysis techniques in this paper have benefits to both the planning and operational aspects of power grid. For planning, our approach can be coupled with the NERC-CIP standards to identify defensive strategies that ensure protections mechanisms are economically allocated to best protect the system. The proposed methodology for substation ranking addresses systematic contingency along with NERC-CIP. This substation ranking based on cost- effectiveness which is important from the view of economic constraint. Furthermore, ability to prioritize the importance of cybersecurity controls ($\alpha_i$), can help utilities prioritize efforts to audit the effectiveness of various control. Utilities must perform period vulnerability assessments of their security mechanisms, however, this process is expensive and time consuming. Therefore, utilities can ensure their efforts are invested into the most critical mechanisms. Furthermore, the proposed techniques can also be used to improve network monitoring by prioritizing efforts on substations which present the highest risk (e.g., lowest $r^s_{aics}$).

Below is the mentioned outcome that are summarized from our above-mentioned case studies and discussions:

- Modeling of the security graph for different IEEE bus system by considering the contingency selection and defensive strategies.
- A complete new set of substation criticality ranking compared to N-1 contingency ranking.
- Component based cybersecurity control ranking that provides a guideline for choosing appropriate security mechanism which needs to be most taken care of. For example, in IEEE 14 bus system, network access control(SCADA) of substation 2 and 4; and system access control of substation 2 are need to be equipped with highly secure software packages.
- Verification of the effectiveness of applying 'Gordon-Loeb' model in our case studies by showing the consistency of cybersecurity control ranking. For example, most of the high critical cybersecurity control ($S_{o,2}$, $S_{vpn2,1}$) are in high impact substation.

The new characteristics introduced by our proposed framework have some cybersecurity adversaries that will affect on the power grid. An attacker could exploit the vulnerabilities of cybersecurity control in the communication network and create impact on the physical system (e.g. Loss of load, manipulating electricity market, etc.) by directing cyberattacks such as data integrity attack, DoS attack, replay attack, etc. For example, by exploiting the authentication mechanism of substation automation, an attacker able to gain access of state estimation. Also, it is possible for an attacker to perform cyberattack on substation automation system through IEC 61850 protocol. This is possible because IEC 61850 uses Ethernet

communication network and most field devices lack proper security mechanisms [27].

## 7 Conclusion

In this paper, we introduced ARCADES, a cybersecurity analysis framework based on graph resistance method that identifies impact for cyberattack (e.g., switching attack such as unplanned circuit breaker trip). ARCADES provides substation and cybersecurity control ranking of a smart grid network that help operator to decide the deployment of appropriate defense mechanism. Our experimental results show that ARCADES presents a new substation contingency ranking which differs from the traditional power contingency ranking. From our experimental result, we also find out that most critical security mechanism located in the high/medium impact substation. While the proposed graph rankings explored unit weights, the model and metrics could easily be extended to include tailored graph edge weights based on a specific utility's confidence in their environment. Furthermore, this work does not attempt to model all controls in a security defense strategy, such as those that focus on the detection of attacks (e.g., intrusion detection systems, audit logs). Future efforts should also explore how detect-oriented controls are incorporated into these models and metrics.

## 8 Ackonwledge

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

## 9 References

1 Electricy Information Sharing and Analysis Center (E-ISAC)/SANS Institute.,' Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case', March, 2016
2 Idaho National Laboratory (INL).,'NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses', May, 2010
3 North American Electricity Reliability Council (NERC).,'NERC Criticial Infrastructure Protection (CIP) Reliability Standards', 2015
4 North American Electricity Reliability Council (NERC).,'NERC CIP-005-5 - Cyber Security - Electronic Security Perimeter', November, 2013
5 Pfleeger, S., Cunningham, R.: 'Why measuring security is hard', IEEE Security Privacy, 2010, 8, (4), pp. 46–54
6 Patapanchala, P. S., Huo, C., Bobba, R. B., Cotilla-Sanchez, E.: 'Exploring Security Metrics for Electric Grid Infrastructures Leveraging Attack Graphs', IEEE Conference on Technologies and Sustainability, Phoenix, AZ, USA, April, 2016
7 Chopade, P., Bikdash, M., :'New centrality measures for assessing smart grid vulnerabilities and predicting brownouts and blackouts', International Journal of Critical Infrastructure Protection, 2016, 12, pp. 29–45
8 Hahn, A., Govindarasu, M.,:'Cyber Attack Exposure Evaluation Framework for the Smart Grid',IEEE Transactions on Smart Grid, 2010, 2,(4), pp. 835–843
9 Dacier, M., Deswarte, Y., Kaniche, M.: 'Quantitative assessment of operational security: Models and tools', LAAS Research Report, 964493, May, 1996
10 Dacier, M., Deswarte, Y.:'Priviledge graph: An extension to the typed access matrix model', Proc. European Symp. Research in Computer Security, 1994, pp. 319–334
11 Wang, L., Singhal, A. , Jajodia, S. : 'Toward Measuring Network Security Using Attack Graphs', Proceedings of the ACM workshop on Quality of protection, 2007.
12 LeMay, E., Ford, M. D., Keefe, K., Sanders, W. H., Muehrcke, C.: 'Model-based security metrics using adversary view security evaluation (advise)', Eighth International Conference on Quantitative Evaluation of Systems (QEST), September, 2011, pp. 191–200
13 P. Manadhata, P., Wing, J. :'An attack surface metric', IEEE Transactions on Software Engineering, June, 2010.
14 Wang, L., Jajodia,S., Singhal, A., Cheng, P., Noel, S. :'k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities', IEEE Transactions on Dependable and Secure Computing, 2014, 11, (1), pp30–44
15 Ten, C.-W., Manimaran, G., Liu, C. C-.,: 'Cybersecurity for Critical Infrastructures: Attack and Defense Modeling', IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, November, 2008, 23, (4),pp. 1836–1846
16 Kundur,D., Feng, X., Liu,S., Zourntos, T., ButlerPurry,k.,: 'Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid', IEEE SmartGridComm, 2010.
17 Zonouz,S.A., Berthier,R., Khurana,H., Sanders, W.H., Yardley,T. :'Seclius: An information flow-based, consequence-centric security metric', IEEE Transactions on Parallel and Distributed Systems, February, 2015, 26, (2),pp. 562–573, Feb 2015.
18 J. Stamp,J., McIntyre,A., Ricardson,B.,: 'Reliability impacts from cyber attack on electric power systems', IEEE/PES Power Systems Conference and Exposition,Seattle, May,2009,pp. 1-8
19 Oman, P., Schweitzer,E., Roberts, J. :'Safeguarding IEDs, substations, and SCADA systems against electronic intrusions', In: Proceedings of the 2001 western power delivery automation conference, 2001, pp. 9–12,
20 Vellaithurai, C., Srivastava, A., Zonouz, S., Berthier, R.,:'CPIndex:cyber-physical vulnerability assessment for power-grid infrastructures', IEEE Transactions on Smart Grid, March , 2015, 6, (2), pp. 566–575
21 Zonouz, S., Davis, C. M., Davis, K. R., Berthier, R., Bobba, R. B., Sanders, W. H.,:'Socca: A security-oriented cyber-physical contingency analysis in power infrastructures', IEEE Transactions on Smart Grid, January, 2014, 5, (1), pp. 3–13
22 Xiang, Y., Wang, L., Yu, D., Liu, N.,: 'Coordinated attacks against power grids: Load redistribution attack coordinating with generator and line attacks', IEEE Power Energy Society General Meeting, July 2015, pp. 1–5
23 Ernster, T. A., Srivastava, A. K.,: 'Power system vulnerability analysis towards validation of centrality measures' , IEEE PES transmission and distribution conference and exposition, 2012
24 Verendel, V.,: 'Quantified security is a weak hypothesis: A critical survey of results and assumptions', In Proceedings of the ACM Workshop on New Security Paradigms , New York, NY, USA, 2009, pp. 37–50
25 National Institute of Standards and Technologies (NIST): 'Framework and roadmap for smart grid interoperability standards âĂŞ release v3.0' (NIST Special Publication, Gaithersburg, MD, 2014)
26 Pacific Northwest National Laboratory (INL).,'Securing Wide Area Measurement Systems', June, 2007
27 Wang, W., Lu, Z.: 'Cybersecurity in the smart grid: survey and challenges', Comput. Netw., 2013, 57, (5), pp. 1344–1371
28 North American Electricity Reliability Council (NERC),: 'NERC CIP-005-5 - Cyber Security - Electronic Security Perimeter', November 2013
29 North American Electricity Reliability Council (NERC),: 'NERC CIP-007-5 - Cyber Security - Systems Security Management', November 2013.
30 North American Electricity Reliability Council (NERC),: 'NERC CIP-003-7 - Cyber Security - Security Management Controls', October 2014.
31 North American Electricity Reliability Council (NERC),: 'NERC CIP-002-1 - Cyber Security - Critical cyber assets identification', June 2006.
32 North American Electricity Reliability Council (NERC),: 'NERC Reliability Concept-version 1.0.2' , December, 2007.
33 Ten, C. W-., Liu, C. -C, Manimaran, G.,: 'Vulnerability Assessment of Cybersecurity for SCADA Systems'. IEEE Transactions on Power Systems, July, 2010, 40, (4), pp. :853–865
34 Gordon, L, Loeb, M.,: 'The economics of information security investment', ACM Transactions on Information and System Security(TISSEC), 2002.
35 Gordon, L., Loeb, M., Lucyshyn, W., Zhou,L.: 'Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model', J. Inf. Secur., 6, January 2014, pp. 24âĂŞ30
36 Hughes, J.,: 'Harmonization of IEC 61970, 61968, and 61850 Models', Electric Power Research Initiative (EPRI), December, 2006
37 Bompard, E., Pons, E.,Wu, D.,:'Extended topological metrics for the analysis of power grid vulnerability',IEEE Syst. J., September, 2012, 6, (3),pp. 481–487 '
38 Estrada, E., Hatano, N.,: 'Resistance Distance, Information Centrality, Node Vulnerability and Vibrations in Complex Networks', Network Science,Springer, December 2010, pp. 13–29.
39 Klein, D. J., Randic,M.,: 'Resistance distance', Journal of Mathematical Chemistry, December 1993, 12, (1), pp. :81–95
40 North American Electricity Reliability Council (NERC),: 'Guidance for Secure Interactive Remote Access' , July, 2011.
41 Univ. Washington,: 'Power Systems Test Case Archive', Seattle, WA,USA.