Electric Power Systems Research 235 (2024) 110769

Contents lists available at ScienceDirect

Electric Power Systems Research

journal homepage: www.elsevier.com/locate/epsr

# Cyber-Physical Modeling and Vulnerability Assessment of Substations for Transmission System Operator☆

Shashank S. [a,*], Gurunath Gurrala [b], P.S. Sastry [b], Vaibhav Katewa [a]

[a] Department of Cyber Physical Systems, Indian Institute of Science, Bengaluru, India
[b] Department of Electrical Engineering, Indian Institute of Science, Bengaluru, India

ARTICLE INFO

*Keywords:*
Bus-branch model
Common information model
Cyber–physical energy systems
Node-breaker model
Vulnerability assessment
Substation configuration

ABSTRACT

In bulk power systems, the majority of interaction between cyber and physical components takes place in substations. However, in most of the cyber–physical power system models the physical layer is typically done using the bus-branch (BB) model, where each substation is considered as a single node. This approach will not capture the details of the cyber layer. This paper proposes a framework to model the substations using node-breaker (NB) models for physical system representation so that the detailed station configurations, the current and the voltage transformer positions, arrangements of protective relays, bay control units and associated communication infrastructure within the substations and its dependencies on the physical elements can be captured effectively using a single cyber–physical graph. Keeping a transmission system operator in view, who does not use power flow and security assessment tools for station operations and maintenance, a vulnerability assessment approach is proposed to assess the risk using some representative attack scenarios. The proposed approach is demonstrated using WECC 3-machine system for breaker and half station configuration. The attack scenarios are developed based on the real substation configuration and the adversary's ability to understand the substation protection and BI/BO operations.

## 1. Introduction

Bulk power networks are one of the largest man-made, strongly coupled cyber–physical systems. The physical layer consists of electrical and control equipment that are deployed at the substations and transmission lines. The cyber layer consists of intelligent electronic devices (IED) with communication and networking equipment. The physical layer sends the measurements and status data of various control equipment through the cyber layer. The cyber layer analyses the data, takes decisions and sends control commands back to the physical layer [1]. Several approaches have been followed to model the physical layer, cyber layer and the cyber–physical interactions. A review of various modeling approaches is presented in [2,3].

A graph theory based cyber–physical inter-dependency model is developed in [4], to study the cascading failures on the overall network. It uses a random network model to represent both physical and cyber networks with a 1:1 dependency mapping between the two layers. The Information and Communication Technology(ICT) and Electric Power Grid(EPG) vulnerabilities, given incomplete information is addressed in [5]. A real-time aurora-like event is modeled to demonstrate a cyber–physical attack and the impact is analyzed using information theory based topology measure. In [6], the routers and control center are modeled as communication nodes. The cyber–physical dependency is modeled at two levels. First, it is assumed that each communication node receives power from exactly one physical node in the distribution grid. The physical nodes in the distribution system are powered by available nodes from the transmission system. A load control policy is used to study the cascading effect of failures. The sensors on breakers that would send information to the control center through the routers are also modeled in [7]. The cyber–physical interactions are modeled by defining a unique type of channel for each type of information device and the physical layer. Vulnerability assessment is done under different types of cyber attacks such as DoS, replay attacks. In [8], the physical layer is modeled considering each substation as a node and the communication layer is built as a scale-free network using network growth algorithm. Two approaches of cyber–physical interfacing is presented based on the properties, degree-betweenness and closeness centrality. The vulnerability assessment is carried out by studying the

☆ This work was supported by POWERGRID Centre of Excellence in Cyber Security, IISc, Bengaluru, India under the project titled "Modeling and Vulnerability Assessment of Power Grids". We acknowledge fellowship support of the Centre for Networked Intelligence (a Cisco CSR initiative) at IISc, Bengaluru.

* Corresponding author.
*E-mail addresses:* shashanks1@iisc.ac.in (Shashank S.), gurunath@iisc.ac.in (G. Gurrala), sastry@iisc.ac.in (P.S. Sastry), vkatewa@iisc.ac.in (V. Katewa).

https://doi.org/10.1016/j.epsr.2024.110769
Received 1 October 2023; Received in revised form 17 April 2024; Accepted 17 June 2024
Available online 4 July 2024

consequence of failure of cyber node on the physical side operations by running optimal power flow. A stochastic-geometry-based power grid model is developed in [9]. A degree-based coupling is done with the communication nodes. Cascading failure simulation is applied to identify the nodes with the greatest damage impact.

The electrical properties of the network are modeled using the centrality measures to assess the vulnerability at the physical layer in [10]. The communication network is modeled in [11] as a hierarchical network with the grid side sensors, ICT backbone network and control center. It studies the load distribution over a period of time and does a vulnerability assessment based on weighted centrality indices at the communication layer. SCADA system is included in [12] for the communication layer modeling. Cyber attacks against the SCADA are modeled using semi-Markov process. It presents a framework to compute mean time-to-compromise and loss of load probabilities to provide a vulnerability assessment. In [13] the communication network is modeled considering one IED at the substation level, a firewall which can be accessed through the control center using different services. Each substation's communication unit is mapped to the corresponding physical node. In [14], detailed communications infrastructure within a substation including SCADA system, IEDs, routers is considered. Both [13,14] use the Common Vulnerability Scoring System to assign a probability for the cyber-attack. The Impact on the physical side is quantified based on load loss by performing a DC power flow based contingency analysis. However, they do not consider substation configuration and practical protection philosophies and their interactions being implemented for reliability purposes.

In [15], the importance of Node-Breaker representation of the physical power system network for planning and transient-stability studies for utilities was discussed. In this paper, we make an attempt to model bulk power systems including substations using node-breaker models. Algorithms for obtaining the physical graph from BB-model data or from a CIM model are provided. Algorithms are developed for getting a communication graph from BB-model data or IEC61850 based station configuration description (SCD) file of a substation. The connections between physical and cyber systems are added through the current transformers (CT), voltage transformers (VT/PT) and switching devices status signals as per the physical substations, and is used to obtain the cyber–physical graph of the entire system. WECC 3-machine system is used to implement the proposed CPS model for different station configurations assumed at all the buses. It is shown that the size of the cyber–physical graph increases significantly while capturing the interactions among all the elements as per realistic implementation, including redundancy.

If the entire system data is available, the corresponding cyber–physical impacts can be quantified using any of the vulnerability methods in the literature. However, transmission systems operators (TSO) who run the substations and associated transmission lines do not use energy management system functions such as operator power flow, state estimation and security assessment tools. They remotely operate substations based on the grid operator's commands and do routine maintenance schedules. They will have measurements and the maximum ratings of the assets and highest privileges in accessing the substation infrastructure remotely. We calculate the probability of software vulnerability using the exploitability measure from the CVSS score. The results of vulnerability analysis for the WECC 3-machine system are provided.

The major contributions of this paper are as follows:

- This paper proposes a framework to model the substations using node-breaker (NB) model for physical system representation so that the detailed station configurations, CT and VT positions, arrangements of protective relays, bay control units and associated communication infrastructure within the substations and their interactions with the physical elements can be captured effectively using a single cyber–physical graph.

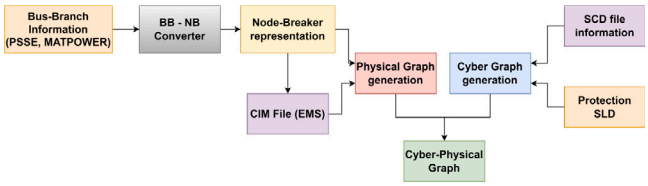



**Fig. 1.** Proposed cyber–physical modeling framework.

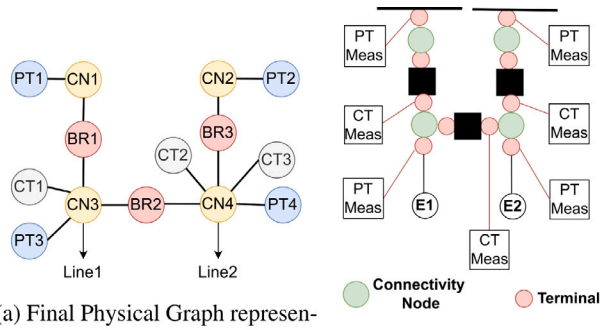
- Substation and system level impact factors are proposed for assessment of the consequence of cyber attack.
- A vulnerability assessment framework based on CVSS score is proposed utilizing the proposed impact factors for TSOs.
- Two attack models are discussed, considering the adversary's knowledge on the substation protection and BI/BO operations.
- The proposed framework is implemented on WECC 3-machine system and the results of the risk analysis for the developed attack scenarios are presented.
- The importance of securing the IED placement information in substations (i.e. SCD files) and usage of the programmable BI/BOs in IEDs is highlighted.

## 2. Cyber–physical modeling

Our overall modeling framework is shown in Fig. 1. Physical electrical system information typically exists as a BB model data file (PSSE or MATPOWER format) or as an NB model in a standard Common Information Model (CIM) file used in the Energy Management Systems (EMS). If the input is MATPOWER data [16], it is first converted to a node-breaker representation using an algorithmic approach described in [17]. Under our modeling framework, we add the CTs and PTs as graph nodes. In any modeling framework, the series elements such as transmission lines, transformers are modeled as edges of the graph. The CB is also a series element; however, it has status and control information exchange with the IEDs, which are modeled at the cyber layer. Similarly CTs and PTs exchange measurements with the IEDs. In our graph model CBs, CTs and PTs are modeled as graph nodes as they directly get connected to IEDs. This helps us preserve the interactions between protection cyber elements and the CB, CT and PT. Sources, loads and shunt elements are modeled as nodes. All the elements are connected to intermediate nodes, called connectivity nodes (CN). The busbar is considered as a CN, instead of a separate graph node. Since a reference CIM file is not available for the WECC 3-machine system, the NB representation is converted to a CIM file. From the CIM file, the physical topology is extracted to obtain a graph representation as described in Algorithm 2. The physical layer graph of the electrical system can also be directly obtained from the NB model as described in Algorithm 1. The communication architecture and the cyber–physical interactions can be obtained from the IEC-61850 standard based substation configuration description (SCD) file [18] or in conventional substations it can be obtained from the protection logic single line diagrams (PSLD). In this paper, we present Algorithm 3 and Algorithm 4 to model the communication network. The former approach involves building of the communication network using the MATPOWER BB file based on a set of standard protection schemes used practically at the substation [19]. In the latter approach, we develop a parser to extract communication network infrastructure graph from SCD file. Both the physical and cyber graphs are combined into a single graph by extending the IEDs connections to the CBs, CTs and PTs, capturing all the cyber–physical interactions as described in Fig. 3.

### 2.1. Physical layer modeling

Several Node-Breaker configurations are practiced at the substations [20]. Under our modeling framework, we consider three config-




(a) Final Physical Graph representation

(b) CIM based graph for BAH

**Fig. 2.** Proposed graph models.

urations for transmission substations: Main and Transfer Bus (MTB), Breaker and Half (BAH), and Double Bus Double Breaker (DBDB). For the generating substations, we consider a Single Bus Single Breaker scheme. A representative diagram for 1 dia of a substation under BAH is shown in Fig. 3. We present two approaches for modeling of the physical power system network — Algorithm 1 uses the algorithm presented in [17] and adds the station elements, CT and PT information in the physical graph representation. Algorithm 2 uses CIM XML data file as input. A CIM based graph representation with the CIM objects connectivity nodes and terminals proposed in [21] is used for generating CIM graph in Fig. 2(b). Both the algorithms generate a graph representing the final physical NB topology model of the system as output is shown in Fig. 2(a).

**Algorithm 1** MATPOWER BB Data File to NB Physical Graph Conversion

**Input(s):** MATPOWER case file, config data file
**Output:** A Graph representing the NB Topology model of the System

Use algorithm presented in [17] and obtain the NB representation of the system.
The variables and incidence names are used as per the cited paper, with a change in labeling convention.
$Mat^{phy}_{adj}$ denotes the adjacency matrix of physical system.
Each node can be labeled as per implementation.
Compute required number of CTs and PTs
$N^{st}_{ct} = N^{st}_{br}$
$N^{st}_{linept} = N^{st}_{ele}$
$N^{st}_{buspt} = N^{st}_{phy}$
Build the final Physical topology Model from NB representation as follows:

**for** $i \leftarrow 1, N_{st}$ **do** ▷ Topology within the substation
  Create edge between Bus PTs and corresponding bus CN
  **for** $j \leftarrow 1, N^{st}_{phy}$ **do** ▷ For each bus $Mat^{phy}_{adj}[BusPT\_i\_j][BusCN\_i\_j] = 1$
  **end for**
  **for** $j \leftarrow 1, N^{st}_{dia}$ **do**
    **for** $k \leftarrow 1, N^{st}_{ct}$ **do** ▷ Bay level
      Create edge between CTs and corresponding element CN $Mat^{phy}_{adj}[CT\_i\_j\_k][EleCN\_i\_j\_k] = 1$
    **end for**
    **for** $k \leftarrow 1, N^{st}_{linept}$ **do**
      Create edge between Line PTs and corresponding element CN $Mat^{phy}_{adj}[LinePT\_i\_j\_k][EleCN\_i\_j\_k] = 1$
    **end for**
  **end for**
**end for**
Make the final Adjacency Matrix symmetric (we assume undirected edges) and output the final physical graph as $Mat^{phy}_{adj}$.

The XML tag 'Substation' in the CIM file is used to identify a particular substation in the network. The VoltageLevel and Bay sections under each substation hold the bay level elements information within a substation. The XML file is parsed to obtain the section-level information. The Terminal element information forms the key source of connectivity as it contains all the associated Power System elements under consideration in our framework (BusBar, Breaker, series, source or shunt) and also defines the Connectivity Node that it is attached

**Algorithm 2** CIM file to Physical Graph

**Input(s):** CIM XML file
**Output:** A Graph representing the NB Topology model of the System

Parse the CIM XML file to extract $< Substation >$ tags
The unique CIM rdfid of each element can be used as graph node label.
$Mat^{phy}_{adj}$ denotes the adjacency matrix of physical system.
**for** $i \leftarrow 1, N_{Sub}$ **do**
  Read $< Terminal >$ tag information
  CN = GetrdfValue("Terminal.ConnectivityNode")
  Create a graph node corresponding to the CN
  **for all** Attr == Terminal.ConductingEquipment **do**
    CE = GetrdfValue("Terminal.ConductingEquipment")
    Create a graph node corresponding to the element
    Create an edge between the element and the Connectivity Node $Mat^{phy}_{adj}[CN][CE] = 1$
  **end for**
**end for**
Make the final Adjacency Matrix symmetric (we assume undirected edges) and output the final physical graph as $Mat^{phy}_{adj}$.

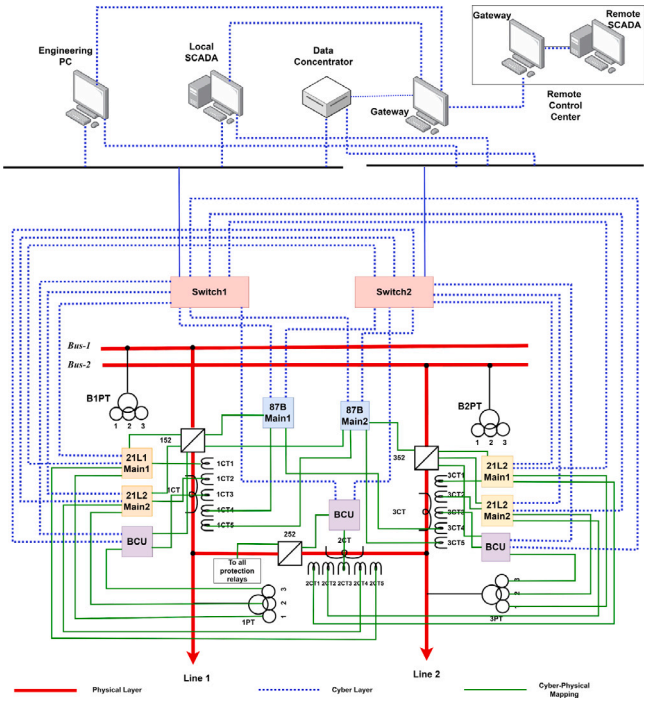



**Fig. 3.** Cyber–physical interactions for BAH.

to. The Connectivity Node has a reference to the Bay and hence the Substation. With the attributes of the Terminal tag information consisting of elements and connectivity node information, we will be able to create a graph representation similar to Fig. 2(a) which is the final output of the algorithm. The algorithms are self-explanatory.

### 2.2. Cyber layer modeling

The cyber layer is made up of components that read the data from the physical layer and make decisions on the operations of the physical layer. The interactions of the cyber and physical layer are shown in Fig. 3 for a BAH station. The conventional substations use different types of IEDs to capture information from the physical components and transmit to further levels at the hierarchy, local SCADA at substation level and the remote control center SCADA. An engineering PC, containing different manufacturers' software for configuration and updation of the IEDs is hosted, and a data concentrator to periodically retrieve data from IEDs and fault recorders, are deployed at

the substation level. The switches provide the datapath to facilitate dataflow between protection devices and the substation level systems with redundancy on different local area networks (LAN). In our communication layer modeling framework, we have considered all the protection devices, engineering PC, local gateway, remote gateway and the remote center SCADA as graph nodes. The communication links between them are represented as edges. The substation-level data flow and communication is assumed to be governed by IEC 61850 standard [22]. However, the framework is generic for any other protocols. There are different class of IEDs based on their protection function — Line distance protection (21L), Transformer Differential protection (87T), Overcurrent protection (67), BusBar differential protection (87B), Generator differential protection (87G) etc. A Bay Control Unit (BCU) is used to control a particular CB section including the associated isolators and earth switches, called bay in a substation. BCU is also used for metering purposes. As per the guidelines by Central Electricity Authority (CEA) of India [23], for transmission systems above 220 kV, each feeder or bus side must be protected by two protection units Main-1 and Main-2. These two protection functions generally manifest in two different physical relays which comprise of different operating principles and different vendors. In our modeling framework, we have considered the following protection devices including redundancy as per CEA for each transmission substation:

- For a transmission line, the protection devices associated are distance protection relays. Two relays of different manufacturers Main1 and Main2.
- For an Inter-connecting Transformer (ICT) element, the associated protection devices are transformer differential protection with overcurrent protection relays of different manufacturers Main1 and Main2.
- Bay Control Unit is used for protection at each bay and does metering functionality. No redundancy for BCUs.
- A centralized busbar protection scheme with busbar protection relays of different manufacturers Main 1 and 2.

The modeling can be easily extended to other elements such as generating substations, distribution substations and associated protection systems.

#### 2.2.1. Algorithm: Cyber layer modeling using MATPOWER data file

For modeling of the cyber layer we use either MATPOWER data file or SCD file. The type of the feeder line and the number of dia per substation act as key inputs. In the substation configuration file, we maintain information as to whether an interconnecting branch is a transmission line type or ICT type element. Once the NB model is obtained, the IEDs can be populated bay-wise as per the PSLD. Algorithm 3 gives an approach for the development of the cyber graph from MATPOWER file.

#### 2.2.2. Algorithm: Cyber layer modeling using SCD file

Substation Configuration Description (SCD) file provides information on the communication configuration of a substation of the power system network. It is an XML-based document which is defined using the IEC 61850 standard based Substation Configuration Language (SCL) [24]. The tags or sections of the SCD file that are under consideration for our modeling framework are Substation, ConnectedAP and IED. The Substation section consists of details of the substation including voltage levels, bays and associated IEDs. Each communicating device has an IP address defined under the ConnectedAP section. The IED section has details on all the Logical Node (LN)s present in an IED and also the Inputs subsection of the IED section captures all the inputs to a given IED. Using the information available from the SCD file, Algorithm 4 describes the procedure to build the cyber network from the SCD file.

**Algorithm 3** Cyber Model from MATPOWER BB file

**Input(s):** MATPOWER case file, config data file
**Output:** Cyber Topology model of the System
Use algorithm presented in [17] and obtain the NB representation of the system.
$Mat^{cy}_{adj}$ denotes the adjacency matrix of cyber system.
Compute the number of protection relays per substation $N_i^{LD}$, $N_i^{DF}$, $N_i^{BCU}$, $N_i^{BB}$, $N_i^{OC}$, $N_i^{GP}$, $N_i^{LP} = 0$
**for** $j \leftarrow 1, N_{Se}$ **do** ▷ consider the Series elements
  **if** type = Transmission **then** $N_i^{LD}$ += 2
  **else** $N_i^{DF}$ += 1 $N_i^{OC}$ += 1
  **end if**
**end for**
Add generator protection units for Source elements
**for** $j \leftarrow 1, N_{Se}$ **do** $N_i^{GP}$ += 2
**end for**
Add load protection units for load
**for** $j \leftarrow 1, N_{Sh}$ **do** $N_i^{LP}$ += 2
**end for**
$N_i^{BCU} = N_i^{Br}$ ▷ 1 BCU per breaker
$N_i^{BB} = 2$
The labeling of cyber layer node is left to the implementation.
**for** $i \leftarrow 1, N_{Sub}$ **do** ▷ Topology within the substation
  Associate each of the relay elements with Engineering PC:
  **for all** Protection Relay R **do** $Mat^{cy}_{adj}$[R][$E_{PC}$] = 1
  **end for** $Mat^{cy}_{adj}[E_{PC}][L_{GW}] = 1$
  Connect the Local GW with the Remote GW $Mat^{cy}_{adj}[L_{GW}][R_{GW}] = 1$
**end for**
Connect remote Gateway and SCADA $Mat^{cy}_{adj}[R_{GW}][R_{SCADA}] = 1$
Make the final Adjacency Matrix symmetric (we assume undirected edges) and output the final physical graph as $Mat^{cy}_{adj}$.

**Algorithm 4** Build Cyber Model from SCD file

**Input(s):** SCD files of substations
**Output:** Cyber Topology model of the System
obtain the value of number of Substations in the network as $N_{st}$
**for** $i \leftarrow 1, N_{st}$ **do**
  Obtain the IED:IP address mapping using the $< ConnectedAP >$ section of the SCD file
  Create nodes for each IED using the above information
  **for all** IED under $< IED >$ tag **do**
    **for all** InputIED **do** $Mat^{cy}_{adj}$[IED][InputIED] = 1
    **end for**
  **end for**
  Connect IEDs to the Engineering PC as described in Algorithm 3
**end for**
Connect to the Remote Center as described in Algorithm 3
Make the final Adjacency Matrix symmetric (we assume undirected edges) and output the final physical graph as $Mat^{cy}_{adj}$.

### 2.3. Cyber–physical interfacing

The Cyber–Physical mapping captures the interactions between the Physical and Cyber components. The Physical and Cyber topology graphs built using the techniques described above are used to form a single graph that includes all the Physical, Cyber nodes, edges and the interconnections between the physical and cyber layers. At the Physical layer side, CTs, PTs and Breakers are the elements that participate in the Cyber–Physical interactions. On the Cyber side, IEDs, BCUs participate in the Cyber–Physical interactions. Each CT is assumed to have 5 cores and PTs are assumed to have 3 cores. Under these assumptions, The Cyber–Physical interactions are represented in Fig. 3. The modeling of these interactions is shown in Algorithm 5.

The results of applying Algorithms 1, 3, 5 on the WECC 3-machine system for BAH, DBDB and MTB substation configuration schemes are shown in Table 1. The BB model data is compared for reference. It can be observed that the physical graph vertices and edges considerably increase due to NB modeling. The proposed CPS-graph accurately captures the exact interactions between the cyber and physical elements because the edges and nodes exactly represent the realistic arrangements in the substations. The algorithms provide a logical description of how the graphs can be built, they cannot be described to exactly to produce a code because of space limitations.

**Table 1**
Modeling results for WECC 3-machine system.

| | Physical Graph | Cyber Graph | Cyber–Physical Graph |
|---|---|---|---|
| Bus-Branch Model | 15 Vertices<br>18 Edges | 15 Vertices<br>18 Edges | 30 Vertices<br>54 Edges |
| Node-Breaker Model<br>(Breaker and Half) | 181 Vertices<br>186 Edges | 98 Vertices<br>97 Edges | 281 Vertices<br>697 Edges |
| Node-Breaker Model<br>(Double Bus Double Breaker) | 174 Vertices<br>198 Edges | 98 Vertices<br>97 Edges | 272 Vertices<br>709 Edges |
| Node-Breaker Model<br>(Main and Transfer Bus) | 144 Vertices<br>144 Edges | 98 Vertices<br>97 Edges | 242 Vertices<br>655 Edges |

**Algorithm 5** Build Cyber–Physical Model using Physical and Cyber graphs

**Input(s):** Physical, Cyber graphs of the network, Bay level information and data generated during Physical and Cyber graph generation.
**Output:** Cyber–Physical model of the System

**for** $i \leftarrow 1, N_{Sub}$ **do** ▷ Under each substation
  **for** $j \leftarrow 1, N_i^{Bay}$ **do** ▷ For each Bay
    Associate the Breaker with a BCU protection relay
    Associate the Central core of CT with the BCU
    Read the type of branch - Transmission or ICT line
    **if** type = Transmission **then**
      Associate the CT, Line PT cores 1 and 2 with Distance protection Main 1, Main 2 respectively
      Associate Line PT core 3 with the BCU
      Associate Breaker with Distance relays Main 1, Main 2
    **else**
      Associate the CT cores 1 and 2 with Differential protection and Overcurrent protections respectively.
      Associate Bus PT core 1 with the Overcurrent protection
      Associate Bus PT core 3 with the BCU
      Associate Breaker with Differential protection and Overcurrent protection
    **end if**
  **end for**
  **if** $C_i$ = BAH and Bay = tieline **then**
    Associate CT cores 1 and 2 with the protection units associated with Line 1
    Associate CT cores 4 and 5 with the protection units associated with Line 2
    Associate breaker with the protection units associated with Lines 1 and 2
  **end if**
  Associate all the Breakers with Busbar protection units.
**end for**

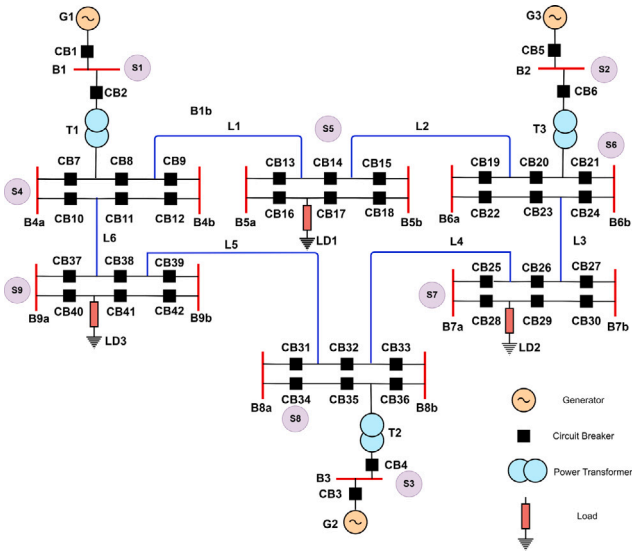



**Fig. 4.** Node-Breaker representation of the WECC system.

## 3. Vulnerability assessment

Under the proposed vulnerability assessment framework, we study the impact of a possible cyber-attack on the power system. The end goal of an adversary is to affect the operations of the physical power system. It could be in the form of preventing a protection function from operating when intended, i.e. during a fault or could be in the form of unwanted breaker operations which will disable electrical components during operations. Depending on the expertise level of the adversary, various scenarios are possible. We quantify the probability of attack and also its impact on the physical side. The final risk index is defined as $\mathbf{R_i} = \mathbf{P_i} * \mathbf{C_i}$, where $\mathbf{R_i}$ is the risk index of $i$th scenario, $\mathbf{P_i}$ is the probability of attack and $\mathbf{C_i}$ is the consequence of the attack on the Physical layer.

### 3.1. Vulnerability assessment of physical power system network

A node breaker representation of the WECC 3-machine system is shown in Fig. 4. The system has two types of transmission substations (TSS): stations connected to generation substations (through a transformer) and two transmission lines (S4, S6 and S8) and stations connected to a load and two transmission lines (S5, S7 and S9). Our goal is to define the impact of the loss of physical assets from the transmission operator's perspective, as they do not use any EMS tools for system-level analysis. We assume that the TSO has access to real-time measurements from all the substations within his jurisdiction and their maximum electrical capacities in MVA. Based on this, we define the element impact factor for each electrical element (transformer, line, load) within a substation, denoted by $IF^1_{ele}$ as follows:

$$IF^1_{ele} = \frac{P_{ele}}{\sum_{ele=1}^{n} S^{MAX}_{ele}}$$

where $P_{ele}$ is the real power MW flowing through the line and $S^{MAX}_{ele}$ is the MVA power capacity of the element. $n$ indicates the number of elements within the substation. This information can be computed at scheduled time intervals (e.g. hourly or after major changes in schedules) based on the power flow measurements at that point in time. This index gives the impact of an element with respect to the maximum capacity of the station. In practice, the line flows may be well below the rated conditions; thus, the impact factors will be very small. In such cases, the following index can be used, which is completely based on the $P, Q$ measurements as follows:

$$IF^2_{ele} = \frac{P_{ele}}{\sum_{ele=1}^{n} S_{ele}}$$

If measurement data is not available or dynamic change in the index is not desired, we can use just the capacities of the elements as follows:

$$IF^3_{ele} = \frac{P^{MAX}_{ele}}{\sum_{ele=1}^{n} S^{MAX}_{ele}}$$

For the substations under the purview of TSO, we also define the impact factor as:

$$IF_{sub} = \frac{P_{sub}}{\sum_{sub=1}^{n} S^{MAX}_{sub}}$$

$$where\ S^{MAX}_{sub} = \sum_{ele=1}^{n} S^{MAX}_{ele}\ and\ P_{sub} = \sum_{ele=1}^{n} P_{ele}$$

**Table 2**
Impact of loss of each element and overall substation under WECC 3-machine system.

| Substation (Elements) | Transmission line 1 | | Transmission line 2 | | Transformer/Load | | Substation | |
|---|---|---|---|---|---|---|---|---|
| | local | system | local | system | local | system | local | system |
| Substation 4 (L1, L6, T1) | 6.146 | 0.95 | 8.192 | 1.266 | 14.391 | 2.224 | 28.729 | 4.439 |
| Substation 5 (L1, L2, LD1) | 7.879 | 0.95 | 15.243 | 1.837 | 23.118 | 2.786 | 46.24 | 5.573 |
| Substation 6 (L2, L3, T3) | 14.861 | 1.837 | 6.027 | 0.745 | 21.25 | 2.627 | 42.138 | 5.209 |
| Substation 7 (L3, L4, LD2) | 5.961 | 0.745 | 18.791 | 2.348 | 24.748 | 3.093 | 49.499 | 6.186 |
| Substation 8 (L4, L5, T2) | 15.198 | 2.348 | 17.301 | 2.673 | 32.6 | 5.037 | 65.099 | 10.058 |
| Substation 9 (L5, L6, LD3) | 17.017 | 2.673 | 8.057 | 1.266 | 25.042 | 3.934 | 50.116 | 7.873 |

indicate the maximum capacity of the substation and actual power flow within the substation respectively. Similar to elements, one can also define two other impact factors for substations that are based on maximum power flows. We have computed the $IF^1_{ele}$ by running the power flow for the WECC 3-machine system and the impact factors of each element and substations are shown in Table 2. It can be noted that the same transmission line has different impact under different substations using local scores based on the rating of the particular substation. $IF^1_{ele}$, $IF^2_{ele}$, $IF^3_{ele}$ and $IF_{sub}$ are defined as local measures within a substation. We also define same metrics at system level by using a system level parameter $S^{MAX}_{System}$ as denominator in all these metrics instead of a local value. It is defined as

$$S^{MAX}_{System} = \sum_{sub=1}^{n} S^{MAX}_{sub}$$

The impact factor for all the elements and substations at system level is also shown in Table 2. The impact factors are represented as percentage values, so that the risk index values do not become too small. The impact factor results indicate that the importance of elements and substations using local and global measures are consistent. At system level, same line at different stations has the same impact factor. The line and transformer capacities of WECC 3-machine system considered in MW are $\{L1-L6, T1-T3\} = \{166.6, 99.9, 99.9, 166.6, 166.6, 166.6, 166.6, 166.6, 200\}$. For the loads 30% higher than the base power flow case is considered as the max MVA rating.

### 3.2. Impact assessment of protection and control system

As per the typical protection and control system architecture adopted for the paper shown in Fig. 3 the Engineering PC (E-PC) is the only cyber entity that has a direct communication with all the IEDs through configuration tools. The external communication with E-PC is secured using a gateway firewall. Each substation sends the data to the remote control center. For our study, we focus on the substation level communication architecture.

#### 3.2.1. Protection mechanism of relays

Each relay hosts a set of protection functions. These functions are defined by the IEC61850 standard and have a defined set of actions that they represent. The CEA guidelines [23] state that the transmission line feeders must be provided with the following minimum set of functions: Distance protection (PDIS, 21), back-up Directional phase over current (PDOC, 67), earth fault protection (PDEF, 67N), Over voltage protection (PTOV, 59), Local breaker back-up protection (RBRF, 50BF) and Under voltage protection (PTUV, 27). Similarly, the busbar protection must have Differential protection (PDBF, 87B) function at minimum. During the fault, the primary functions act, in case the main protection function fails the backup protections will act. The protection functions can either directly trip the circuit breaker coil through the Trip (TP) command or issue initiate protection (IP) commands to invoke other protection functions. There exists an electromechanical relay called the master trip relay that can be initiated via a direct trip command by the backup protection functions to trip the circuit breaker. There are binary inputs (BI) and binary outputs (BO) on the relay, through which the control signals (IP) or commands (TP) are received and sent respectively. The exact number of such BI/BO ports can vary as per the station requirements. In this paper, we assume that there are 16 BIs and 16 BOs in each IED.

#### 3.2.2. Common vulnerability scoring system (CVSS)

CVSS is a vendor-agnostic, industry open standard maintained by Forum of Incident Response and Security Teams (FIRST). For a known vulnerability under the common vulnerabilities and exposures (CVE) databse, the CVSS scoring system assigns a risk score. The base metric consists of two sub-metric groups — Exploitability and Impact. The exploitability score reflects the ease and technical means by which the vulnerability can be exploited. Impact score reflects the direct consequence of a successful exploit. In this paper, we propose to use only the exploitability score as the probability of attack metric. A search on the CVE database with the keyword 'SCADA' lists the following vulnerabilities that are published in 2023 until September 15th: CVE-2023-{4986, 4985, 4485, 0956, 3329, 2866, 2187, 2186, 30459, 41976, 1256, 0595, 22611, 22610}. The remote control center PC hosts a remote SCADA system (R-SCADA), a set of softwares and services for monitoring and control. If exact SCADA details on the R-SCADA system are available then one can get all the relevant CVSS scores. Here we assume only the above listed SCADA vulnerabilities on the R-SCADA. With the listed vulnerabilities, the average exploitability score of gaining access to the R-SCADA of a control center is obtained as 2.9. To make the exploitability score normalized, we divide it by the maximum possible exploitability score under the CVSS 3.1 framework, which is 3.9. The probability of exploiting the vulnerabilities and gaining access to the R-SCADA of a control center, denoted by $P^{exp}_{R-SCADA}$ is obtained as 0.74. For an actual system, this exploitability from CVSS scores can be obtained by doing an audit of the vulnerabilities of the OS, accessibility services (FTP, HTTP, SSH etc..) and other installed software on the R-SCADA system. An attacker can trigger CB operations right from the operator console of the R-SCADA with high certainty if the access control to HMI is compromised. So the probability of an attack on R-SCADA for this scenario is as follows:

$$Prob^{attack}_{R-SCADA} = P^{exp}_{R-SCADA} * P^{HMI-Access}_{R-SCADA}$$

The consequence of this would be very severe as the attacker can cause multiple substations to go down. However, we assume that the operators can easily discover this scenario as the remote control centers are operated 24/7. So, the consequence and risk of this scenario is not explored further in this paper.

### 3.3. Probability of attack on the substation

The focus of the paper is on the vulnerability assessment within a substation and hence we consider the scenarios where an attacker can gain access to the E-PC or local SCADA system (L-SCADA) of a substation by exploiting the vulnerabilities on the R-SCADA system. There may be several layers of access controls between E-PC, L-SCADA and R-SCADA, then the whole path need to be considered in the assessment. The probability of gaining access and exploiting from R-SCADA can be obtained from CVSS scores as explained above for R-SCADA. However, for simplicity we assume that the attacker will be able to successfully access Engg. PC or L-SCADA if attacker is able to exploit R-SCADA. So, the probability of gaining access and exploiting Engg. PC, L-SCADA i.e. $P^{exp}_{E-PC}$, $P^{exp}_{L-SCADA}$ from R-SCADA are treated as 1. One can also consider a direct attack using the resources within the substation to get access to Engg. PC or L-SCADA. Our framework is general and can be extended to multiple attack paths.

#### 3.3.1. Exploiting vulnerability on the remote control center SCADA to gain access to the local SCADA

Once the adversary successfully exploits the vulnerabilities on the R-SCADA, the attacker can gain access to a L-SCADA in a substation by exploiting its vulnerabilities. In L-SCADA, attacker can operate CBs by directly sending commands from the local operator console (HMI) and can cause unwanted tripping of the entire substation with certainty. So the probability of attack on a L-SCADA can be obtained as follows:

$$Prob^{attack}_{L-SCADA} = P^{exp}_{R-SCADA} * P^{exp}_{L-SCADA} * P^{HMI-Access}_{L-SCADA}$$

It can be observed that additional layers of access to R-SCADA or L-SCADA HMI can reduce the probability of attack. The timeout features of HMI are not being used or bypassed typically in some control centers for ease of operations. We strongly recommend to use these features with strong passwords.

#### 3.3.2. Exploiting vulnerability on the remote control center SCADA to gain access to the engineering PC

After successfully exploiting the vulnerabilities on the R-SCADA, an adversary can gain access to an E-PC in a substation by exploiting its vulnerabilities. As discussed above $P^{exp}_{E-PC} = 1$ is assumed in these discussions. This attack scenario is of importance because E-PC is used for all the IED configurations. Many IED manufacturers allow different modes of operation of the IEDs, such as test mode, deployment mode, configure mode etc. through their custom software. We assume that these tools can be opened to access and configure IEDs without strong access control measures. So the probability of IED access from E-PC is assumed as 1. We elaborate two attack models through which IEDs can be compromised in the following sub-sections.

### 3.4. Cyber attack on the IEDs within a substation

Once the E-PC is compromised, we focus our study on the substation-level communication architecture. We define Main1 (M1) and Main2 (M2) together, corresponding to the same protection relay function (21 or 87), as one protection unit. For any transmission substation under the WECC 3-machine system, with BAH scheme, there will be one protection unit for each element (line/trafo/reactor/load), one protection unit for busbar protection and one BCU for each CB. In general, the number of IEDs including the BCUs in a given substation, denoted by $N^{IED}_{Sub}$ can be deduced by the formula:

$$N^{IED}_{Sub} = 2 * (N^{Ele}_{Sub} + 1) + N^{Br}_{Sub}$$

where, $N^{Ele}_{Sub}$ indicates the number of electrical elements (loads, transformer, line, reactor) in the substation, and $N^{Br}_{Sub}$ indicates the number of breakers in the substation. In case of WECC 3-machine system, under BAH scheme, there are 14 IEDs (4-21L, 2-87B, 6-BCU, 2–87 for trafo/reactor/load) each under the transmission substations S4–S9. We define the number of IEDs based on their type as follows: $N^{Prot-IED}_{Sub} = 2{*}N^{Ele}_{Sub}$, $N^{Prot-BB}_{Sub} = 2$ and $N^{BCU}_{Sub} = N^{Br}_{Sub}$. where $N^{Prot-IED}_{Sub} = N^{Dist}_{Sub} + N^{T/L/R}_{Sub}$ indicates the number of protection IEDs other than busbar, $N^{Dist}_{Sub}$ denotes the number of distance relays corresponding to the lines, $N^{T/L/R}_{Sub}$ denotes the number of differential relays corresponding to the transformer or loads or reactors, $N^{Prot-BB}_{Sub}$ indicates number of busbar protection IEDs and $N^{BCU}_{Sub}$ indicates the number of BCUs within a substation. We assume that the adversary cannot access the IEDs simultaneously as the attacker has to open the corresponding software specific to the manufacturer and compromise the IEDs one after the other. We make a key assumption that the adversary has a limited time of access before his actions are discovered, and can access and modify a maximum of two relays one after the other. For the IEDs getting compromised, we present two attack models, Attack Model-I (AM-I) and Attack Model-II (AM-II), based on what the adversary can do if attacker gains access to an E-PC.

### 3.5. Attack model — I: Unwanted tripping of CBs leading to contingencies

In this attack model we assume that the attacker somehow knows the use of IED software to give trip commands from BCUs, distance/differential and busbar protection relays to the associated CBs through their BO outputs. We consider the following two scenarios based on the knowledge of the attacker about substation protection.

#### 3.5.1. Scenario-1: The attacker does not have knowledge of substation protection

If an attacker cannot distinguish protective relays and BCUs of different manufacturers attacker needs to try every IED randomly for tripping the elements. Depending on the time attacker has and the number of relays attacker can access within the available time, the impact can be $N-1$, $N-2$ or any higher order contingencies or the loss of entire substation. In the WECC 3-machine system, $N-1$, $N-2$ and loss of entire substation are the possible contingencies in the S4-S9 substations. Under the assumed BAH scheme, by tripping both the main and the tie CB of an element an $N-1$ contingency can be deliberately created. The adversary can gain access to any one of the protection IEDs (M1 or M2) or both the main and tie BCUs to send out signals to open a circuit breaker associated with the element. With the stated assumptions, there are 4 ways in which an $N-1$ contingency can be caused. The attacker gains access to any one protection IED to trip the associated breakers with a probability of $\frac{N^{Prot-IED}_{Sub}}{N^{IED}_{Sub}} * \frac{1}{N^{Ele}_{Sub}}$, or the attacker gains access to two BCUs corresponding to the same element with a probability of $\frac{N^{BCU}_{Sub}}{N^{IED}_{Sub}} * \frac{1}{N^{IED}_{Sub}-1} * \frac{1}{N^{Ele}_{Sub}}$, or attacker gains access to a BCU in the first try, and in the subsequent try gains access to a protection IED with a probability of $\frac{N^{BCU}_{Sub}}{N^{IED}_{Sub}} * \frac{N^{Prot-IED}_{Sub}}{N^{IED}_{Sub}-1} * \frac{1}{N^{Ele}_{Sub}}$, or attacker gains access to the busbar protection IED and trips the associated breakers with a probability $\frac{N^{Prot-BB}_{Sub}}{N^{IED}_{Sub}} * \frac{1}{N^{Ele}_{Sub}}$. For an $N-2$ contingency, the adversary has to gain access to at least one IED in each protection unit corresponding to the two different elements with a probability of $\frac{N^{Prot-IED}_{Sub}}{N^{IED}_{Sub}} * \frac{N^{Prot-IED}_{Sub}-2}{N^{IED}_{Sub}-1} * \frac{1}{N^{Ele}_{Sub_{C_2}}}$, or has to gain access to the busbar protection IED with a probability $\frac{N^{Prot-BB}_{Sub}}{N^{IED}_{Sub}} * \frac{1}{N^{Ele}_{Sub}}$. If there are $N$ elements in the station the $N-1$ contingency due to each element is equally probable. Similarly, there are $N_{C_2}$ different pairs of elements that can cause $N-2$ contingency in the station and each such instance is equally probable. So, in the above probability computations $\frac{1}{N^{Ele}_{Sub}}$ and $\frac{1}{N^{Ele}_{Sub_{C_2}}}$ factors can be seen with $N-1$ and $N-2$ contingencies respectively. Finally, attacker can cause the entire substation to go down by accessing any one busbar protection IED to open all the associated breakers with a probability of $\frac{N^{Prot-BB}_{Sub}}{N^{IED}_{Sub}}$. Based on the above probabilities, we can compute the probability of attack using AM-I with no protection knowledge as follows:

$$Prob^{S1}_{AM-I} = P^{exp}_{R-SCADA} * P^{contingency}_{AM-I}$$

where $contingency$ refers to $N-1, N-2$ or the entire substation as discussed above.

#### 3.5.2. Scenario-2: The attacker has knowledge of substation protection

If the attacker has knowledge of substation protection i.e. attacker can distinguish protective relays (21L, 87T, 87B etc.) and BCUs of different manufacturers, then the attacker can cause entire substation collapse by just using the bus-bar relays to trip the CBs with certainty. So the probability of attack using AM-I with protection knowledge is given by (see Table 3).

$$Prob^{S2}_{AM-I} = P^{exp}_{R-SCADA}$$

**Table 3**
Probability of causing contingencies under AM-I.

| Contingency | Using busbar protection IED | Using element protection IED | Using BCU | Using BCU and element protection IED | Probability of attack |
|---|---|---|---|---|---|
| $N-1$ (Scenario-1) | 0.048 | 0.143 | 0.011 | 0.066 | 0.198 |
| $N-2$ (Scenario-1) | 0.048 | 0.044 | – | – | 0.068 |
| Substation down (Scenario-1) | 0.143 | – | – | – | 0.106 |
| Substation down (Scenario-2) | 1 | – | – | – | 0.74 |

### *3.6. Attack model — II: Prevention of protection functions from operating when they are intended to*

After gaining access to the protection IEDs, the adversary can perform a set of tasks to disable the intended protection functionality of the device and disable the protection mechanism from operating at the time of a fault. The probability associated with fault is not considered in this work. We believe that this kind of attack cannot be detected by the operators easily. This kind of attack can cause physical damage to the equipment and would take a longer time to restore the system. The different ways in which this can be done with increasing level of difficulty as per our assessment are:

- Disable the protection functions
- Inhibit the BI/BO ports
- Modify the settings in the relay
- Modify the protection algorithm in the relay

The last two actions require a good deal of expertise in terms of understanding manufacturer-specific configurations, ICT tools and the protection mechanisms. Such an expertise is difficult to obtain for an external adversary. We present various scenarios with varying levels of the adversary's expertise and analyze the impact for the first two cases. Some manufacturers allow configuration, settings change, trip and close commands of relays through terminal access. However, some manufacturers require loading of the configuration file via ftp (file transfer protocol) for any changes. Here we assume that the adversary has knowledge of how to perform these actions.

#### *3.6.1. Disable the protection functions of a protection IED*

Once the adversary has gained access to a protection IED, attacker can start disabling the protection functions present in them by sending out a command. To be able to achieve this, it is assumed that the adversary has a complete knowledge of the protection functions operating on the relay and the attacker is not randomly disabling them. The attacker can distinguish protective relays of different manufacturers to inhibit the protection. In a physical substation, there could be several relays of same type and make protecting different elements. So having the knowledge of relay placement is important in addition to the knowledge of protection functions. We present the following two possible scenarios.

#### *3.6.2. Scenario 1: Attacker knows relay placement and has the knowledge of protection functions*

The adversary is an expert on the protection functionalities. Plus, attacker is aware of the relay arrangement in the substation. Under such a case, the adversary can definitively attack designated relays and compromise the intended protection functions. Thus the probability associated with this attack scenario is only the probability of gaining access to the R-SCADA system. Let us denote the probability for this scenario to be $Prob^{S1}_{AM-II}$ and it is given by:

$$Prob^{S1}_{AM-II} = P^{exp}_{R-SCADA}$$

#### *3.6.3. Scenario 2: Attacker does not know relay placement but has knowledge of protection functions*

The adversary is an expert on the protection functionalities. However, the attacker is not aware of the relay arrangement in the substation. The attacker can only get a sense of distance or differential relays but does not know which line they protect, or whether the selected differential relay is used for transformer, load, reactor or bus bar protection. The adversary has to first gain access to both the Main-1 and Main-2 protection IEDs corresponding to an element. For the distance protection unit, it is sufficient for the adversary to disable PDIS (Distance Protection) function and PDEF (Directional Earth fault) functions which will prevent the initiation of the Breaker failure protection too. The probability of disabling any one protection unit can be obtained as, the probability of choosing a distance unit $Prob^{access}_{Dist-unit} = \frac{N^{Dist}_{Sub}}{N^{Dist}_{Sub}} * \frac{1}{N^{Dist}_{Sub}-1} * \frac{1}{N_{Lines}}$ of any one line or the probability of choosing a differential unit corresponding to a transformer/load/reactor $Prob^{access}_{T/R/L} = \frac{2}{N^{T/L/R}_{Sub}+N^{Prot-BB}_{Sub}} * \frac{1}{N^{T/L/R}_{Sub}+N^{Prot-BB}_{Sub}-1} * \frac{1}{N_{T/L/R}}$. Since attacker can compromise only two relays one after the other as per our assumption, this selection will result in $N-1$ contingency only. Attacker can make a choice of either distance or differential to be disabled with certainty. If there are $N$ elements in the station the $N-1$ contingency due to each element is equally probable. So a factor $\frac{1}{N_{Lines}}$ and $\frac{1}{N_{T/L/R}}$ is used in the probability calculations. However, if attacker selects busbar unit then the entire substation protection can be disabled with a probability of $Prob^{access}_{BB} = \frac{2}{N^{T/L/R}_{Sub}+N^{Prot-BB}_{Sub}} * \frac{1}{N^{T/L/R}_{Sub}+N^{Prot-BB}_{Sub}-1}$. Based on the above probabilities we can compute the probability of attack using AM-II, scenario-2 as follows:

$$Prob^{S2}_{AM-II} = P^{exp}_{P-SCADA} * Prob^{S2}_{disable}$$

where $Prob^{S2}_{disable} = Prob^{access}_{Dist-unit}$ if chooses distance, $Prob^{S2}_{disable} = Prob^{access}_{T/R/L}$ if chooses other elements for $N-1$ and $Prob^{S2}_{disable} = Prob^{access}_{BB}$ for the entire substation down. In the Scenarios 3–6 below we assume that the adversary has no knowledge on the protection functions.

#### *3.6.4. Inhibit binary outputs/inputs of IED*

The control and the initiation commands from the relays are sent as electrical signals through the binary output ports (BO). Each BO is designated to send a particular signal which carries either a trip command or a signal to initiate other protection functions. The protection mechanism fails when all the BI or BO ports that correspond to the primary and the secondary protection functions are inhibited from operating. In case of a BAH scheme, there are eight BOs and one BI on the distance protection unit that needs to be blocked to prevent any possible protection mechanism operating on the main and tie circuit breakers. The signals that are involved in the line distance protection are: A breaker trip to main CB coil 1, 2, tie CB coil 1, 2, Master trip main CB, tie CB, breaker fail initiation for main CB, tie CB and a direct trip channel receive for Main CB. One key assumption is that the BI/BO contact is either a Normally Closed (NC) or a Normally Open (NO) contact. Hence, just sending a '0' does not ensure that the BI/BO port is disabled. It depends on the type of contact. The adversary needs to send a '0' or '1' trying to disable a particular BI/BO port, but cannot be sure of successful blocking of the port. If all the BI/BOs are of same type (NO/NC) the attack is trivial. So we strongly recommend IED manufacturers to use mixed contacts for BI/BOs. With 9 such BI/BOs involved with line distance protection, there are $2^9$ possible combinations if mixed contacts are used. Out of these, we found that 16 cases lead to an N-1 contingency, 32 cases lead to an N-2 contingency and 48 cases lead to the entire substation going down. With these attack models and assumptions, we describe various attack scenarios in detail.

**Table 4**
Probability of causing contingencies under AM-II.

| Scenarios | Contingencies | Prob(Prot. IED access) | Prob(BIBO access) | Prob(attack) |
|---|---|---|---|---|
| Scenario 1 | $N-1$ | 1 | – | 0.74 |
| | $N-2$ | | – | |
| | Substation down | | – | |
| Scenario 2 | $N-1$ | 0.167 | – | 0.123 |
| | $N-2$ | 0 | – | 0 |
| | Substation down | 0.167 | – | 0.123 |
| Scenario 3 | $N-1$ | 1 | 0.001 | 0.001 |
| | $N-2$ | | 0.004 | 0.003 |
| | Substation down | | 0.009 | 0.007 |
| Scenario 5 | $N-1$ | 0.167 | 0.001 | 0.0001 |
| | $N-2$ | 0.167 | 0.004 | 0.0005 |
| | Substation down | 0.167 | 0.009 | 0.001 |

#### 3.6.5. Scenario 3: Attacker knows relay placement and has some knowledge of BI/BO

The adversary has insider information on the relay placement and has expertise on the relay BI/BO ports. The attacker can distinguish protective relays of different manufacturers. With an intention of preventing the protection mechanism from working as intended, the attacker starts blocking the BI/BO ports. He knows that there are 9 BI/BO ports that are involved in the protection function but does not exactly know whether a '0' or a '1' will block them. Here we assume only 21L BI/BO being inhibited. However, attacker need to do this for the entire protection unit (M1 & M2). The probability associated with this scenario involves the probability of gaining access to the R-SCADA system and the probability of compromising the known BI/BO combinations of a unit that lead to an impact. Let us denote the probability for this scenario to be $Prob^{S3}_{AM-II}$ and it is given by:

$$Prob^{S3}_{AM-II} = P^{exp}_{R-SCADA} * (Prob^{inhibit}_{BIBO})^2$$

The $Prob^{inhibit}_{BIBO}$ for $N-1$, $N-2$ and substation down contingencies are given in Table 4 using a 21L.

#### 3.6.6. Scenario 4: Attacker knows relay placement but does not have the knowledge of BI/BO

The adversary has insider information on the relay placement but does not have expertise on the relay functions or mechanisms, although the attacker can distinguish protective relays of different manufacturers. With an intention of preventing the protection mechanism from working as intended, attacker has to block the BI/BO ports randomly, as a single '0' or '1' vector is not an option. The probability associated with this scenario involves the probability of gaining access to the R-SCADA system and compromising the BI/BO combinations that lead to an impact. Given that out of $2^{32}$ BI/BO combinations, there are only 96 that cause an impact, the $Prob^{inhibit}_{BIBO}$ value is 2E-8 for one distance relay, which is close to 0. This scenario is practically infeasible. Let us denote the probability for this scenario to be $Prob^{S4}_{AM-II}$ and it is given by:

$$Prob^{S4}_{AM-II} = P^{exp}_{R-SCADA} * (Prob^{inhibit}_{BIBO})^2 \approx 0$$

#### 3.6.7. Scenario 5: Attacker does not know relay placement and has some knowledge of BI/BO

The attacker is an outsider, but has some expertise on the relay BI/BO ports. The attacker cannot block protection functions, but can distinguish protective relays of different manufacturers. Attacker understands what BI/BO ports are responsible for the protection signals, but does not have an exact mapping of the relays to the elements. This scenario is exactly similar to scenario-2 of AM-II with additional task of inhibiting BI/BO ports as attacker cannot disable protection functions. The attacker starts blocking the known BI/BO ports of distance relay one by one to prevent the protection operations from action. The probability associated with this scenario involves the probability of gaining access to the R-SCADA system, the probability of choosing an entire distance protection unit $\frac{2}{N^{Dist}_{Sub}}$ and the probability of compromising the known BI/BO combinations that lead to an impact given in Table 4. Let us denote the probability for this scenario to be $Prob^{S5}_{AM-II}$ and it is given by:

$$Prob^{S5}_{AM-II} = P^{exp}_{R-SCADA} * Prob^{access}_{Dist-unit} * (Prob^{inhibit}_{BIBO})^2$$

#### 3.6.8. Scenario 6: Attacker does not know relay placement and does not have the knowledge of BI/BO

The adversary is an outsider and has no expertise on the relay BI/BO ports, cannot block protection functions, but the attacker can distinguish protective relays of different manufacturers. The attacker starts blocking the BI/BO ports randomly. As discussed previously, Overall, 96 cases have an impact on the operations. The probability associated with this scenario involves the probability of gaining access to the R-SCADA system, the probability of gaining access to an entire unit of distance protection relay and the probability of compromising the BI/BO ports that lead to an impact similar to scenario-4 whose value is 2E-8. This scenario is practically infeasible. Let us denote the probability for this scenario to be $Prob^{S6}_{AM-II}$ and it is given by:

$$Prob^{S6}_{AM-II} = P^{exp}_{R-SCADA} * Prob^{access}_{Dist-unit} * (Prob^{inhibit}_{BIBO})^2 \approx 0$$

### 3.7. Results

Under the Risk assessment framework, the Risk Index scores for each scenario on the WECC 3-machine system at a substation level and system level is presented in Table 5 for AM-I and AM-II. For each substation under each scenario, we compute the consequences using the impact scores for $N-1$ contingency, $N-2$ contingency and the loss of entire substation. These impact scores are taken from Table 2. Finally the risk index for each substation is computed as the product of the probability of attack and the consequence. Scenarios 4 and 6 in AM-II are not considered as their practical impact is negligible. From the Table 5, it can be observed that both the local and system level risk scores preserve the severity order for the elements within a substation and across the substations. Scenario-2 in AM-I and scenario-1 in AM-II are practically same and have the highest risk. However, we believe that in the latter case, the damage caused by inhibiting the protection when needed will be permanent and will be difficult to detect. It can also be observed that in both the models, whenever the information about the placement of the relays is unknown to the attacker, even though the attacker is knowledgeable in substation protection, the risk is considerably lower. Hence we suggest to keep this information secure and confidential. Typically SCD files contain this information about the stations, which can be secured. Whenever, BI/BOs use mix of NO/NC combinations, the risk is considerably lowered despite the knowledge of relay placement. So programmable BI/BO ports with ability to configure them as NO or NC will significantly reduce the risk. We believe that the proposed framework becomes very handy to create an automated what-if scenarios and vulnerability dashboards for TSO control centers.

**Table 5**
Risk Index results for various scenarios.

| Attack Scenarios | Substation (Lines) | Risk Index at substation level | | | | Risk Index at system level | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | $N-1$ contingency on line 1 | $N-1$ contingency on line 2 | $N-2$ contingency | Substation down | $N-1$ contingency on line 1 | $N-1$ contingency on line 2 | $N-2$ contingency | Substation down |
| Attack Model I — Unwanted trip of CBs | | | | | | | | | |
| Scenario-1: the attacker has no knowledge of substation protection | S4 (L1, L6) | 1.216 | 1.621 | 0.972 | 3.037 | 0.188 | 0.250 | 0.150 | 0.469 |
| | S5 (L1, L2) | 1.559 | 3.016 | 1.567 | 4.888 | 0.188 | 0.363 | 0.189 | 0.589 |
| | S6 (L2, L3) | 2.941 | 1.193 | 1.415 | 4.455 | 0.363 | 0.147 | 0.175 | 0.551 |
| | S7 (L3, L4) | 1.180 | 3.718 | 1.677 | 5.233 | 0.147 | 0.465 | 0.210 | 0.654 |
| | S8 (L4, L5) | 3.007 | 3.423 | 2.202 | 6.882 | 0.465 | 0.529 | 0.340 | 1.063 |
| | S9 (L5, L6) | 3.367 | 1.594 | 1.699 | 5.298 | 0.529 | 0.250 | 0.267 | 0.832 |
| Scenario-2: the attacker has knowledge of substation protection | S4 (L1, L6) | – | – | – | 21.259 | – | – | – | 3.285 |
| | S5 (L1, L2) | – | – | – | 34.218 | – | – | – | 4.124 |
| | S6 (L2, L3) | – | – | – | 31.182 | – | – | – | 3.854 |
| | S7 (L3, L4) | – | – | – | 36.630 | – | – | – | 4.577 |
| | S8 (L4, L5) | – | – | – | 48.173 | – | – | – | 7.443 |
| | S9 (L5, L6) | – | – | – | 37.086 | – | – | – | 5.826 |
| Attack Model II — Inhibit Protection IEDs from operating | | | | | | | | | |
| Scenario-1: the attacker knows relay placement and has knowledge of protection functions | S4 (L1, L6) | 4.548 | 6.062 | 10.610 | 21.259 | 0.703 | 0.937 | 1.639 | 3.285 |
| | S5 (L1, L2) | 5.831 | 11.279 | 17.110 | 34.218 | 0.703 | 1.359 | 2.062 | 4.124 |
| | S6 (L2, L3) | 10.997 | 4.460 | 15.457 | 31.182 | 1.359 | 0.551 | 1.911 | 3.854 |
| | S7 (L3, L4) | 4.411 | 13.905 | 18.316 | 36.630 | 0.551 | 1.738 | 2.289 | 4.577 |
| | S8 (L4, L5) | 11.246 | 12.803 | 24.049 | 48.173 | 1.738 | 1.978 | 3.716 | 7.443 |
| | S9 (L5, L6) | 12.592 | 5.963 | 18.555 | 37.086 | 1.978 | 0.937 | 2.915 | 5.826 |
| Scenario-2: the attacker does not know relay placement and has knowledge of protection functions | S4 (L1, L6) | 0.758 | 1.010 | 0.000 | 3.543 | 0.117 | 0.156 | 0.000 | 0.547 |
| | S5 (L1, L2) | 0.972 | 1.880 | 0.000 | 5.703 | 0.117 | 0.227 | 0.000 | 0.687 |
| | S6 (L2, L3) | 1.833 | 0.743 | 0.000 | 5.197 | 0.227 | 0.092 | 0.000 | 0.642 |
| | S7 (L3, L4) | 0.735 | 2.318 | 0.000 | 6.105 | 0.092 | 0.290 | 0.000 | 0.763 |
| | S8 (L4, L5) | 1.874 | 2.134 | 0.000 | 8.029 | 0.290 | 0.330 | 0.000 | 1.241 |
| | S9 (L5, L6) | 2.099 | 0.994 | 0.000 | 6.181 | 0.330 | 0.156 | 0.000 | 0.971 |
| Scenario-3: the attacker knows relay placement and has some knowledge of BIBO | S4 (L1, L6) | 0.004 | 0.006 | 0.041 | 0.187 | 0.001 | 0.001 | 0.006 | 0.029 |
| | S5 (L1, L2) | 0.006 | 0.011 | 0.067 | 0.301 | 0.001 | 0.001 | 0.008 | 0.036 |
| | S6 (L2, L3) | 0.011 | 0.004 | 0.060 | 0.274 | 0.001 | 0.001 | 0.007 | 0.034 |
| | S7 (L3, L4) | 0.004 | 0.014 | 0.072 | 0.322 | 0.001 | 0.002 | 0.009 | 0.040 |
| | S8 (L4, L5) | 0.011 | 0.013 | 0.094 | 0.423 | 0.002 | 0.002 | 0.015 | 0.065 |
| | S9 (L5, L6) | 0.012 | 0.006 | 0.072 | 0.326 | 0.002 | 0.001 | 0.011 | 0.051 |
| Scenario-5: the attacker does not know relay placement and has some knowledge of BIBO | S4 (L1, L6) | 0.001 | 0.001 | 0.007 | 0.031 | 0.000 | 0.000 | 0.001 | 0.005 |
| | S5 (L1, L2) | 0.001 | 0.002 | 0.011 | 0.050 | 0.000 | 0.000 | 0.001 | 0.006 |
| | S6 (L2, L3) | 0.002 | 0.001 | 0.010 | 0.046 | 0.000 | 0.000 | 0.001 | 0.006 |
| | S7 (L3, L4) | 0.001 | 0.002 | 0.012 | 0.054 | 0.000 | 0.000 | 0.001 | 0.007 |
| | S8 (L4, L5) | 0.002 | 0.002 | 0.016 | 0.071 | 0.000 | 0.000 | 0.002 | 0.011 |
| | S9 (L5, L6) | 0.002 | 0.001 | 0.012 | 0.054 | 0.000 | 0.000 | 0.002 | 0.009 |

## 4. Conclusion

This paper presents a unified cyber–physical modeling and vulnerability assessment framework, including detailed station configurations and practical protection philosophies. Algorithms for BB model to NB model conversion to get physical graph from MATPOWER data file or CIM data file is proposed. Algorithms for obtaining cyber graph from the SCD file is proposed. A single cyber–physical graph including CBs, CTs, PTs and detailed IED arrangements is developed. A vulnerability framework utilizing CVSS scores along with the physical impact factors at local station level and system level, suitable for transmission operators is proposed. The proposed framework is applied to WECC 3-machine system with BAH configuration and the results are presented. A detailed representation of the substation as Node-breaker model facilitates a better understanding of the system at the component-level and an increased granularity in terms of the possible attack models and paths. Two attack models, AM-I and AM-II, with different scenarios based on the attacker's knowledge on the substation protection and BI/BO operations have been proposed. Such an analysis will help the transmission system operator to understand the risk associated with each element in the substation.

## CRediT authorship contribution statement

**Shashank S.:** Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Methodology, Investigation, Formal analysis, Conceptualization. **Gurunath Gurrala:** Writing – review & editing, Supervision, Project administration, Methodology, Funding acquisition, Formal analysis, Conceptualization. **P.S. Sastry:** Validation, Supervision. **Vaibhav Katewa:** Validation, Supervision.

## Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Gurunath Gurrala reports financial support was provided by POWERGRID Center of Excellence in Cyber Security, IISc, Bengaluru and Centre for Networked Intelligence, IISc, Bengaluru.

## Data availability

No data was used for the research described in the article.

## References


[1] V. Aravinthan, et al., Reliability modeling considerations for emerging cyber-physical power systems, in: 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems, PMAPS, 2018.

[2] D. Zhang, et al., A comprehensive overview of modeling approaches and optimal control strategies for cyber-physical resilience in power systems, Renew. Energy (2022).

[3] L. Shi, Q. Dai, Y. Ni, Cyber–physical interactions in power systems: A review of models, methods, and applications, Electr. Power Syst. Res. (2018).

[4] S.V. Buldyrev, et al., Catastrophic cascade of failures in interdependent networks, Nature (2010).

[5] A. Srivastava, et al., Modeling cyber-physical vulnerability of the smart grid with incomplete information, IEEE Trans. Smart Grid (2013).

[6] M. Parandehgheibi, E. Modiano, D. Hay, Mitigating cascading failures in interdependent power grids and communication networks, in: 2014 IEEE Int. Conf. on Smart Grid Communications, 2014.

[7] Y.-n. Wang, et al., On modeling of electrical cyber-physical systems considering cyber security, in: Frontiers of Information Technology and Electronic Engineering, 2016.

[8] J. Guo, Y. Han, C. Guo, F. Lou, Y. Wang, Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties, Energies (2017).

[9] R. Atat, M. Ismail, S.S. Refaat, E. Serpedin, T. Overbye, Cascading failure vulnerability analysis in interdependent power communication networks, IEEE Syst. J. (2022).

[10] E. Bompard, et al., Structural vulnerability of power systems: A topological approach, Electr. Power Syst. Res. (2011).

[11] W. Zhu, J.V. Milanović, B. Mihić, Assessing the applicability of complex network theory models and importance measures to vulnerability studies of cyber-physical systems, in: 2019 IEEE PES Innovative Smart Grid Technologies Europe, (ISGT-Europe), 2019.

[12] Y. Zhang, L. Wang, Y. Xiang, C.-W. Ten, Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation, IEEE Trans. Power Syst. (2016).
[13] H. Lin, L. Shi, Risk assessment of substations in a cyberphysical power system considering attacker's intrusion behavior, in: The 10th Renewable Power Generation Conference, (RPG 2021), 2021.
[14] K. Yan, X. Liu, Y. Lu, F. Qin, A cyber-physical power system risk assessment model against cyberattacks, IEEE Syst. J. (2023).
[15] A. Delavari, et al., Hydro-québec's experience of implementing power-system node-breaker model for planning studies, in: 2021 IEEE 9th International Conference on Smart Energy Grid Engineering, 2021.
[16] R.D. Zimmerman, et al., MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education, IEEE Trans. Power Syst. (2011).
[17] V. Sahu, G. Gurrala, Algorithm to convert power system network data from bus-branch model to node-breaker model, in: 2023 IEEE Power & Energy Society General Meeting, PESGM, 2023.
[18] W. Wimmer, IEC 61850 SCL - More than interoperable data exchange between engineering tools, 2005.
[19] G.K. Palepu, https://gkpalepuprotection.blogspot.com/.
[20] J. Blackburn, T. Domin, Protective Relaying: Principles and Applications, fourth ed., CRC Press, 2014.
[21] G. Ravikumar, S.A. Khaparde, A common information model oriented graph database framework for power systems, IEEE Trans. Power Syst. (2017).
[22] H. Falk, IEC 61850 Demystified, Artech, 2018.
[23] General Guidelines for 765/ 400/ 220/ 132 kV Sub-Station and Switch-yard of Thermal /Hydro Power Projects, Central Electricity Authority, 2012.
[24] R. Mackiewicz, Overview of IEC 61850 and benefits, in: 2006 IEEE PES Power Systems Conference and Exposition, 2006.