# Impact Modeling of DSO-TSO Cross-Domain Fault Propagation Attacks

Mahdi Bahrami and Louis Wehenkel

*Abstract*— **Cross-domain threats are a real challenge for power system operators. While existing research has focused primarily on cyberattacks within either transmission or distribution networks, a critical gap remains in understanding the impacts of cross-domain threats. In response, this paper analyzes coordinated attacks originating from medium-voltage (MV) systems and propagating to high-voltage (HV) transmission systems (TSs) through shared substations. A new approach is proposed to model the possibility of such fault propagation from distribution system operator's (DSO) domain to TS operator's (TSO) domain. The hybrid-attack scenario consists of two sequential steps: 1) manipulating the protection settings of protective devices 2) causing man-made faults on MV feeders. This is formulated as a bilevel optimization problem considering attackers' and TSO's perspective. In addition, the concept of minimal cut-sets is deployed to capture the process of the fault propagation through shared substations. The proposed framework can be used by TSOs as a tool for conducting the impact assessment. The proposed model is tested on the IEEE reliability test system to demonstrate its effectiveness. The simulation results show that the hybrid attacks can lead to significant disruptions, including direct and indirect load shedding, as well as multiple transmission/MV line outages, and hence should be considered by system operators in their security management policies[1].**

***Index Terms*—Bilevel model, cross-domain threats, shared substations, hybrid attacks, minimal cut-sets.**

## NOMENCLATURE

*Indices and Sets*

| | |
|---|---|
| $l, \bar{L}$ | Index and set of transmission lines. |
| $s, \bar{S}$ | Index and set of shared substations between DSOs and the TSO. |
| $p, \bar{I}_s$ | Index and set of protective IEDs at shared substation *s*. |
| $i, \bar{N}$ | Index and set of transmission nodes. |
| $g, \bar{G}$ | Index and set of generating units. |
| $f, \bar{F}_s$ | Index and set of MV feeders at shared substation *s*. |
| $c, \bar{C}_s$ | Index and set of minimal cut-sets at shared substation *s*. |

*Parameters and Constants*

| | |
|---|---|
| $\mathrm{T}_l^{\mathrm{line,max}}$ | Capacity of transmission line *l*. |
| $\lambda_{s,f}^{ph}$ | Resources required for causing man-made fault on feeder *f* of shared substation *s*. |
| $\lambda_{s,p}^{cy}$ | Resources required for manipulating the settings of IED *p* at shared substation *s*. |
| $AR_{ph}$ | Total resources available to attackers for causing man-made faults on MV feeders. |
| $AR_{cy}$ | Total available resources for altering IEDs' protection settings at shared substations. |
| $P_i^{load}$ | Active load demand at node *i*. |
| $x_{l,i-j}$ | Reactance of transmission line *l* connected between nodes *i* and *j*. |
| $\mathbf{B}$ | Susceptance matrix. |
| $P_g^{gen,\min}, P_g^{gen,\max}$ | Lower and upper bounds of power generation of unit *g*. |
| $\tilde{\psi}_c^s$ | Vector of components of minimal cut-set *c* of shared substation *s*. |
| $\zeta_{c,p}^s$ | Binary parameter equal to 1 if IED *p* belongs to minimal cut-set *c* of shared substation *s*. |
| $\zeta_{c,f}^s$ | Binary parameter equal to 1 if feeder *f* belongs to minimal cut-set *c* of shared substation *s*. |
| $\beta$ | Penalty factor. |

*Variables*

| | |
|---|---|
| $\chi_c^s$ | Binary variable equal to 1 if minimal cut-set *c* of shared substation *s* is selected by hybrid attackers. |
| $\mu_{c,f}^s$ | Binary variable equal to 1 if feeder *f* is selected by hybrid attackers in minimal cut-set *c* of shared substation *s*. |
| $\mu_{c,p}^s$ | Binary variable equal to 1 if protective IED *p* is selected by hybrid attackers in minimal cut-set *c* of shared substation *s*. |
| $\mathrm{T}_l^{line}$ | Active power flow on transmission line *l*. |
| $P_g^{gen}$ | Power output of generation unit *g*. |
| $\Delta_g^u, \Delta_g^l$ | Non-negative continuous variables respectively indicating the increase and decrease in power output of unit *g* compared to its original power output before attacks. |
| $P_i^{sh}$ | Amount of load shedding due to any operational violations at node *i* (a.k.a., indirect load shedding) |
| $P_{i,f}^{fsh}$ | Amount of load shedding of feeder *f* due to hybrid attacks against node *i* (a.k.a., direct load shedding) |
| $\varpi_f^s$ | Binary variable equal to 1 if feeder *f* of shared substation *s* is de-energized due to hybrid attacks. |
| $\alpha_l$ | Binary variable equal to 1 if transmission line *l* is de-energized due to hybrid attacks. |
| $\delta_i$ | Voltage phase angle of node *i* (in radians). |

[1] M. Bahrami and L. Wehenkel are with the Department of Electrical Engineering and Computer Science, Montefiore Institute, University of Liège, Liège 4000, Belgium (e-mail: mahdi.bahrami@uliege.be; l.wehenkel@uliege.be).

This work has been prepared with the support of the Belgian Energy Transition Fund, project CYPRESS (https://cypress-project.be/).

## I. Introduction

### A. Motivation and Background

Distribution substations are located at the interface between transmission system operator (TSO) and distribution system operator (DSO) control domains. The transformers connecting distribution and transmission grids delineate the boundaries between the operational domains of TSOs and DSOs [1]. While the transmission side is often well-protected against cyber-intrusions, the distribution systems are often more vulnerable in this respect [2]. Thus, cyber-attackers may attack such shared substations in a way that the transmission system (TS) becomes impacted. For example, during the cyber-attacks on the Ukrainian power systems in 2015, malicious actors targeted three distribution companies [3]. Cross-domain fault propagation attacks can indeed render multiple transmission lines de-energized. System operators should be ready for such threats and, in developing the network code on cybersecurity (NCCS), relevant entities (e.g., ACER, ENTSO-E, and EU DSO Entity, in Europe) should collaborate on this topic [4]. In addition, power system operators require an assessment tool to analyze the possible impacts of cyberattacks.

### B. Literature Review and Research Gaps

In the literature, many studies have focused on the cybersecurity of distribution systems (DSs). However, academic research concerned with the cyber-attacks aiming at impacting TSs from DSs (low-voltage or MV) is scarce. In this category, the few existing research works have mainly focused on cyber-attacks against Internet-of-Things (IoT)-based loads. For example, in [5], the authors propose an optimization model for analyzing the impacts of cyber-attacks against electric vehicle (EV) charging prices on transmission line loading. In [6], a model is proposed to investigate how cyber-attacks on IoT-based devices can propagate from DSs to TSs.

Likewise, in [7] and [8], a framework is proposed to analyze the impacts of load altering attacks (LAAs) on the dynamic response of the power grid. Similarly, the authors in [9] explore the impact of data integrity attacks on solar-based distributed energy resources (DERs) in an integrated distribution and transmission model. Additionally, in the literature, fault propagation caused by attacks in power grids can occur in several ways, including from TS to TS (cross-border) and from DS to TS (cross-domain). While there are a few works focusing on the former [10], [11], the latter has not been addressed. Thus, the two main gaps in research and practice are as follows:

- Cybersecurity of shared substations has not been adequately addressed. This poses challenges for grid operators, because the protection and monitoring schemes are not designed to detect or mitigate cross-domain threats.
- Lack of impact modeling of MV-to-HV fault propagation through shared substations under coordinated hybrid attacks.

Thus, this paper fills these gaps to enhance preparedness for attack scenarios aiming at propagating faults from MV grids to TSs. In addition, our paper is complementary to the studies on cyber-physical attacks on distribution and transmission systems.

### C. Model Description and Scope

This paper is motivated by the research gaps**.** The new research question in this article is: Could fault propagation attacks from MV grids to HV grids (as a cross-domain cyber-attack scenario) through shared substations disrupt the normal operation of transmission systems (TSs)? In this context, this article proposes a novel impact assessment model using minimal cut-sets for the cross-domain hybrid attacks. In this scenario, the attackers launch coordinated hybrid attacks on shared substations, that could most severely disrupt the operation of the transmission system. In the proposed bilevel optimization model, the upper level models the attacker strategy and budget constraints, and the lower level represents the TSO response to the attacks. The hybrid attack consists of two steps: 1) manipulating the protection settings of target protective IEDs at shared substations 2) creating man-made faults on respective MV feeders. To model the fault propagation, the concept of minimal cut-set is utilized. Each minimal cut-set represents a minimal attack path between the MV and the HV sides of a shared substation. Furthermore, the attack resources required for each minimal cut-set are taken into account.

The present study focuses only on impact assessment rather than a full risk assessment which additionally considers the likelihood of such events.

### D. Contributions

The proposed framework allows TSOs to analyze MV-to-HV fault propagation scenarios under different attackers' budget, thereby enabling the most effective TSO response. The main contributions of this paper are as follows:

- Proposing a structured and scalable integration of substation-level protection logic into system-level optimization via minimal cut-set modeling.
- To the best of the authors' knowledge, it is the first framework that models MV-to-HV fault propagation through shared substations.
- The proposed minimal cut-set formulation provides a bridge between detailed substation protection logic and system-level optimization.
- The integration of bilevel optimization with realistic substation topology modeling enables the proposed framework to be applied to any configurations of substations.

### E. Paper Organization

The rest of this paper is organized as follows: Section II introduces the hypothesized hybrid attack scenario under study and discusses the general structure of the proposed framework. Section III presents the threat modeling and its underlying assumptions. The proposed approach for modeling the fault propagation process using the concept of minimal cut-sets is introduced in Section IV. The formulation of the proposed problem is presented in Section V. Subsequently, numerical results are given in Section VI. Finally, Section VII concludes the paper.

## II. Hybrid Attack from MV Grids against TS

In this section, the concept of cross-domain fault propagation from the MV DS to the HV TS is illustrated by an example. Then, the general workflow of the proposed framework is discussed.

### A. Fault Propagation through Shared Substations

To introduce the concept of fault propagation from MV feeders to the TS, the most common configuration of distribution substations (as shared facilities) is used in an illustrative example, as shown in Fig. 1 [12], [13]. In this configuration, each protective IED provides primary protection for a substation component. In addition, a feeder IED provides protection for an MV feeder. In the event of a fault on an MV feeder, the feeder IED acts as the primary protection for the fault. However, if the feeder IED fails to clear the fault, it is isolated by the backup protection scheme. Thus, for the substation shown in Fig. 1, the faulted feeder is isolated by the transformer protection IED. In addition, the protection systems of the incoming transmission lines serve as backup protection for Zone A1 [14]. Thus, this raises a critical question: what happens if both feeder and transformer IEDs cannot see the fault? According to the substation configuration shown in Fig. 1, the backup protection on the incoming transmission line clears the fault [15]. Thus, upon the occurrence of the abovementioned events, the fault on an MV feeder is cleared by the protection system of incoming transmission lines. This can be translated as the fault propagation process from the MV side to the HV side. Because of this process, one or more transmission lines are de-energized.

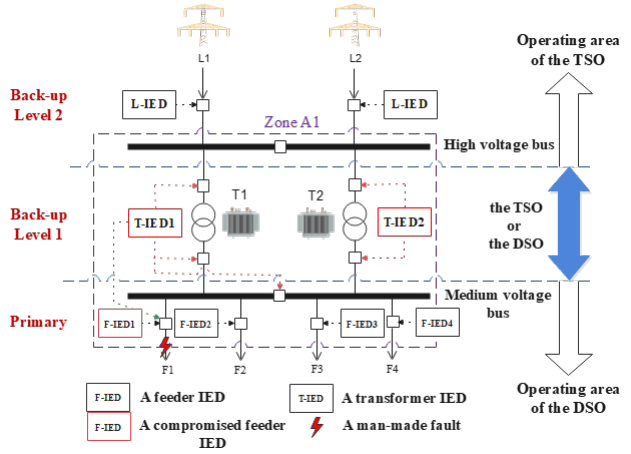


Fig. 1. Topology structure of a typical distribution substation (as a shared substation) [2], [12], as an illustrative example.

### B. Overall Workflow of the Proposed Framework

The overall workflow of the proposed framework is depicted in Fig. 2. The proposed framework consists of two main stages. The first stage, so-called structural analysis, models the shared substation topology and represents its protection logic. Based on the detailed substation configurations, minimal cut-sets that enable fault propagation from the MV to the HV level through shared substations are identified.

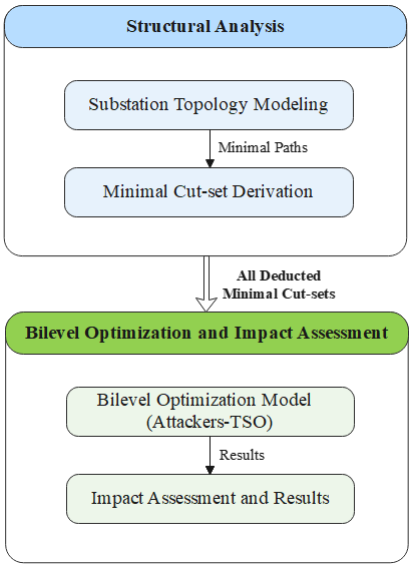


Fig. 2. Overall workflow of the proposed framework.

The second stage, so-called optimization and impact assessment, builds upon the derived minimal cut-sets and takes them as inputs to the bilevel optimization model. To this end, the minimal cut-sets are represented in the form of matrices presented in the Appendix. This representation provides attackers with information on each minimal cut-set, including required attack resources, the affected MV feeders, and the impacted transmission lines. In the optimization model, the upper-level problem models the attackers' decision-making problem. In the upper-level problem, attackers select minimal cut-sets to target transmission lines in order to maximize their objective function. In this process, they consider their attack budget and the TSO's response. The lower-level problem, however, models the TSO's response to such attacks. Subsequently, the resulting problem is solved to quantify the system-level impact of each hybrid-attack scenario in terms of de-energized MV feeders as well as transmission lines, direct and indirect load shedding. This workflow systematically links substation-level structural vulnerability analysis to transmission-level impact quantification.

### C. Cyber Intrusions into Substation IEDs

Protective devices in substations can be accessed through several remote access points [16]. These access points are typically provided by IED vendors for purposes such as remote setting modifications, maintenance, and configuration [17]. In addition, these devices often use standard communication protocols [18]. Furthermore, the majority of IED software can be accessed and downloaded online [19]. Detailed technical documentation for each IED brand and its associated software is available online, making these devices potentially well-known to malicious actors. To illustrate how attackers could exploit vulnerabilities to get access to substation IEDs, two vulnerability reports of substation products published by two different vendors are considered. Some of the information is summarized as [20], [21].

- **Vulnerability cause:** IED1: A bug in OpenSSL 1.0.1c, IED2: Cleartext storage of sensitive

information.

- **Can it be exploited remotely?** IED1: Yes, IED2: Yes.

In such cases, cyber-attackers are able to launch attacks in a stealthy manner. Subsequently, they can modify the settings of IEDs [17].

## III. Threat Model and Assumptions

### A. The Hypothesized Hybrid Attack Scenario

The hypothesized hybrid-attack scenario consists of two sequential steps as follows.

- **Manipulating the shared substation IED settings:** The attackers are assumed to first manipulate IED settings such that the compromised IEDs would not see the man-made faults on MV feeders.
- **Causing man-made faults on MV feeders:** After changing the protection settings of target IEDs, the attackers should cause man-made faults on respective MV feeder(s) of the selected minimal cut-set(s).

According to IEEE 1686, each protective IED is secured with a password [22]. Thus, the process of intruding into an IED is different from other IEDs in a substation.

### B. Assumptions on Attacker Capabilities

The hypothesized hybrid-attack scenario is formulated based on the following assumptions:

- The attackers are assumed to be familiar with IED software programs and substation architecture.
- Cyber-attackers can bypass the security mechanisms of target substations and IEDs.
- Based on the protection configuration of target shared substations, cyber-attackers manipulate all relevant primary protection types (e.g. overcurrent) and their associated backup protections to induce fault propagation.
- The hybrid attackers create three-phase faults on distribution feeders. For overhead lines, this could involve physically bridging conductors through conductive materials, and for underground cables, attackers can access junction boxes to cause short circuits. In addition, they can use chemical corrosive chemical agents that degrade the cable's insulation, thereby creating short circuits within the cable assembly. Furthermore, the man-made faults are created at the points close to the beginning of the targeted feeders. In doing so, the resulting fault current will be high.
- The attackers target the power systems during on-peak hours to put more stress on the grid.
- We conservatively assume a worst-case attacker who can bypass IED protections or initiate physical faults, ensuring that impact quantification remains on the safe side.

### C. Justification for the Hypothesized Hybrid Attack Scenario

There are several justifications for using the hybrid attack strategy against TS, which are listed as follows:

- Such unconventional cyber-physical attack strategies can increase the likelihood of successful attacks, as system operators might not be well enough prepared for such strategies.
- Unlike direct attacks on TS lines, this attack strategy can remain undetected for a longer duration. This is because the fault occurs at MV levels, but it is seen and cleared by the protection system of the TS.
- The hybrid attacks can not only de-energize targeted TS lines and MV feeders but also damage the power transformers whose protection systems have been compromised by the attackers [23].
- The HV and MV grids are managed and operated by two separate entities. Thus, identifying the cause of a protection system operation can be more challenging.

### D. Attack Modeling Limitations

The limitations of the attack modeling approach in this study are summarized as follows:

- **It assumes successful IED manipulation and fault initiation:** The model does not consider detection mechanisms, timing constraints, or operator counteractions.
- **It uses stylized attacker costs and resources:** The attackers' costs and available resources are represented based on common assumptions used in the literature.

### E. Mitigation Considerations and Practical Recommendations

Potential mitigation measures include stricter access control to IED settings, cross-domain monitoring mechanisms, periodic validation of protection configurations, and anomaly detection schemes. In addition, regulatory guidance addressing shared substation cybersecurity could reduce the possibility of such coordinated hybrid attacks. On top of the technical mitigation measures, there is a clear need to strengthen the cybersecurity coordination between the TSO and DSOs. For example, organizations such as ENTSO-E and the EU DSO Entity in Europe have emphasized the importance of cross-border and cross-domain cybersecurity risk assessment, information sharing, and harmonized security requirements for critical grid infrastructures. Shared MV–HV substations represent an interface between different operational domains. Thus, enhanced coordination mechanisms as well as joint contingency analysis could reduce the risk of such hybrid attacks.

## IV. Minimal Cut-set Method

In this section, the concept of minimal cut-set s is introduced. This is followed by an explanation of how this concept is applied in the MV-to-HV fault propagation modeling. The detailed formulation and matrix representation of the minimal cut-sets are provided in the Appendix.

### A. Minimal Cut-set Overview

The cut-set approach is a powerful tool for assessing the reliability of a system. A cut-set is a set of elements, which, when they all fail, leads to system failure [24]. In this context, cut-sets are associated with different failure modes of a system.

This definition implies that a set of components must fail in a way that all possible paths between the input and output of the system are disrupted. However, when only a minimum subset of system components is considered, a cut-set is converted into a minimal cut-set. In this regard, all components of a minimal cut-set must fail so that the system fails. In addition, a minimal cut-set is defined for the components of a path between two points, say input and output [24]. If any minimal cut-set occurs, the system fails. Therefore, minimal cut-sets are schematically connected in parallel.

### *B. Application of Minimal Cut-sets in the Proposed Approach*

In this study, a minimal cut-set is defined between an MV feeder and a transmission line at a shared substation. Thus, for each pair of MV feeder and an incoming transmission line, the minimal cut-sets should be derived. This is repeated for all possible combinations of MV feeders and incoming transmission lines. With this in mind, a minimal cut-set in this study represents a set of man-made faults to be created on MV feeders and the compromised protection devices at the shared substations which, when failed to operate, leads to operation of the protection system(s) on the incoming transmission lines. Thus, a minimal cut-set includes a minimal sub-set of protective devices at shared substations that must fail to operate for propagation of fault(s) from MV networks to the transmission lines. All protective devices of a minimal cut-set must fail to operate for triggering the protection system(s) of incoming transmission lines.

### *C. Outline of the Procedure for Representing MV-to-HV Fault Propagation via Shared Substations as Minimal Cut-sets*

To model which components are impacted by a hybrid attacker scenario, the following steps should be taken:

Step 1: Protection configurations of the shared substations are recognized, including identifying primary and back-up protections for each component.

Step 2: For each of the shared substations, all minimal cut-sets are deduced.

Step 3: For each of the minimal cut-sets identified in Step 2, the directly de-energized transmission lines and MV feeders, the man-made faults and their required resources, the IEDs to be compromised and their required resources are identified.

### *D. The Illustrative Example*

To make the concept clear, we continue with the illustrative example, and thus the approach discussed in the previous part is applied to the substation configuration shown in Fig. 1. In this case, there are four minimal cut-sets, which are shown in Fig. 3. If any of the four minimal cut-sets occurs, the fault in DS is propagated into transmission lines. For example, in the first minimal cut-set, a man-made fault must be caused on MV feeder F1. In addition, the protective IEDs of feeder F1 and transformer T1 must be compromised. Consequently, the man-made fault on F1 is propagated to transmission line L1, and MV feeders F1 and F2 are de-energized, according to the protection configuration of the substation illustrated in Fig. 1. As can be traced in the minimal cut-sets, protective IEDs of transformers T1 and T2 appeared in more than one minimal cut-set.

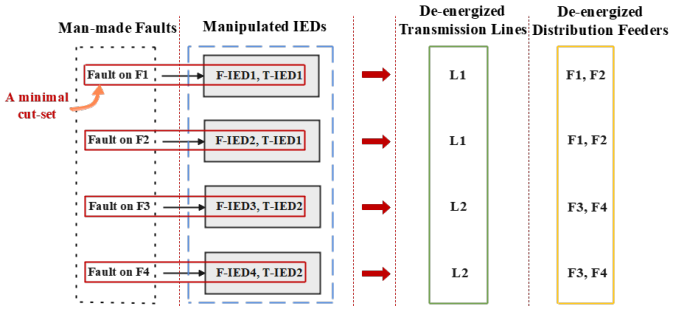


Fig. 3. Minimal cut-sets of the shared substation shown in Fig. 1 and their impacts on the DS and the TS (the illustrative case).

### *E. Minimal Cut-set Deduction*

There are several methods for identifying minimal cut-sets [24], which are mainly based on the concept of minimal paths. The pseudo-code presented in Fig. 4 shows the procedure we have used to identify minimal cut-sets. In the context of this study, each minimal cut-set represents the smallest combination of actions required to propagate man-made faults from the MV network to the HV level through shared substations. These combinations include 1- Manipulation of relevant protection IED settings at the shared substation (e.g., feeder and transformer protections), and 2- Causing man-made faults on selected MV feeder(s).

In this study, a path represents a sequence of network components and associated protection functions that enables fault propagation from the MV side to the HV side of a shared substation. A path is considered *minimal* if it contains the smallest set of MV feeders and IEDs required for such propagation. By constructing the incidence matrix based on minimal propagation paths and iteratively combining attack actions, the algorithm systematically determines the minimal cut-sets. In this regard, the inputs and outputs of the algorithm are:

- **Inputs:** A comprehensive list of all minimal paths connecting an MV feeder to a transmission line through a shared substation. For example, for the illustrative substation shown in Fig. 1, there are 4 minimal paths, which are [{F1, T1}, {F1, T2}, {F2, T1}, {F2, T2}]).
- **Outputs:** The outputs are as a list of sets. We continue with the illustrative example. As shown in Fig. 3, the final minimal cut-sets are: [{F1, F-IED1, T-IED1}, {F1, F-IED1, T-IED2}, {F2, F-IED2, T-IED1}, {F2, F-IED2, T-IED2}]).

```
Algorithm: Minimal Cut-Set Identification

Input: System components and all minimal paths
Output: Minimal cut sets of all orders

1. Identify all minimal paths of the system and store them in Paths.

2. Construct an incidence matrix M:
    - Rows correspond to minimal paths.
    - Columns correspond to system components.
    - M[i,j] = 1 if component j participates in path i, else 0.

3. Initialize CutSets = empty list
   Order = 1

4. Repeat:
   a. For each combination of 'Order' columns in M:
      i. Sum the selected columns element-wise.
      ii. If all entries in the sum are nonzero:
          - The corresponding components form a cut set of current Order.
          - Add this cut set to CandidateCutSets.

   b. Remove from CandidateCutSets any set that contains a lower-order cut set.

   c. Add remaining CandidateCutSets to CutSets.

   d. Increment Order by 1.

5. Until maximum possible Order is reached (or no new cut sets are found)

6. Return CutSets
```

Fig. 4. Pseudo-code for identifying minimal cut-sets.

### F. Final Number of Minimal Cut-sets

In the proposed model, only the substations shared between the TSO and DSOs stand as candidates for disrupting TS. In this regard, minimal cut-sets are formed for such substations. This in turn significantly reduces the computational complexity of the problem.

### G. Cyber-Security Countermeasures

The proposed framework is developed based on the concept of minimal cut-sets. Therefore, it is enabled to incorporate intrusion defense mechanisms. Existing methods, such as artificial intelligence (AI)-based models or graph-based techniques, can be integrated to model cyber intrusions into substation cyber-networks. By employing these approaches, the probability of a successful intrusion into each IED can be estimated. Subsequently, the probability of a successful attack for each minimal cut-set is calculated based on the combined likelihood of compromising the set of components required to disrupt a specific transmission line(s). As a result, different minimal cut-sets targeting the same transmission line(s) may vary significantly in terms of their overall attack difficulty. However, this analysis is beyond the scope of this paper, and this work only focuses on the impact assessment of such attacks on TSs.

## V. Problem Formulation

In this section, the formulation of the bilevel optimization problem is provided.

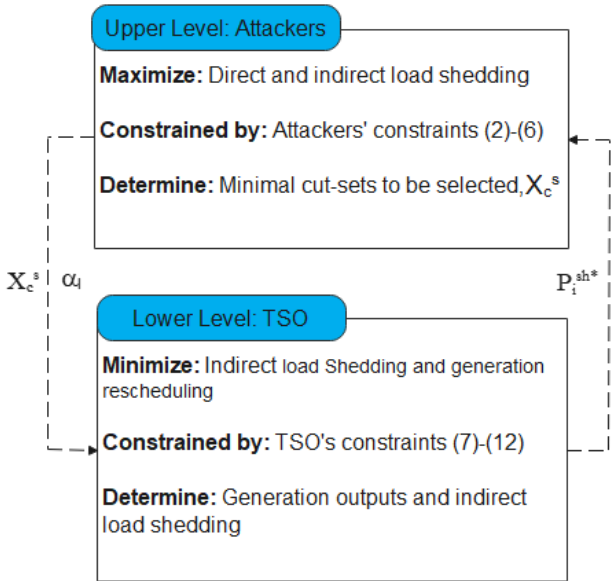


Fig. 5. General overview of the proposed bilevel optimization problem.

### A. General Formulation

The proposed optimization model is a mixed-integer bilevel optimization problem. Furthermore, causing man-made faults that are cleared by the backup protection system already leads to de-energization of some MV feeders at an attacked shared substation, specified by $P_{i,f}^{fed}$ (referred to as direct load shedding) in this work. However, the TSO might have to implement load-shedding program if operational constraints are still violated. Thus, further load might be indirectly shed because of the hybrid attacks, designated as $P_i^{sh}$ (referred to as indirect load shedding). The interaction between the hybrid attackers and TSO in the bilevel optimization model is shown in Fig. 5. This problem is formulated as follows:

$$\begin{aligned} &\underset{\alpha}{Max} \sum_i P_i^{sh*} + \sum_s \sum_{f \in \bar{F}_s} P_{s,f}^{f\,sh} \\ &s.t.: (2)-(6) \\ &P_i^{sh*} \in \arg\min \left\{ \sum_i P_i^{sh} + \beta . \sum_g (\Delta_g^u + \Delta_g^l) \right\} \\ &s.t.: (7)-(12) \end{aligned} \tag{1}$$

The hybrid-attackers' decision-making problem is formulated as the upper level of the proposed bilevel optimization problem. The objective function of the hybrid attackers is to maximize the total amount of load shedding. This objective function is subject to a set of constraints. The lower-lever objective function (TSO's objective) includes two terms. The first term minimizes the amount of load shedding caused by operational violations in the power system. The second one, however, penalizes generation rescheduling. In other words, if there are multiple optimal solutions for the problem, the optimal solution with the lowest magnitude of changes in generation power outputs compared to original ones is selected. Thus, non-negative continuous variables $\Delta_g^u$ (upward changes) and $\Delta_g^l$

(downward changes) are introduced. The lower-level problem depends on the minimal cut sets selected by the cyber-attacker, which are taken as parameters. Moreover, the lower-level objective function is subject to constraints (7)-(12).

*B. Upper-Level Problem*

Given that each minimal cut-set corresponds to an attack resource, these amounts of used resources should be considered in the model. In addition, the resources required for the occurrence of a minimal cut-set is the sum of the resources required for targeting each component of the cut-set. Furthermore, protective IEDs or MV feeders may appear in more than one cut-set as T-IED2 has appeared in minimal cut-sets C3 and C4 in the illustrative example. Nonetheless, the resources for creating man-made fault on an MV feeder or compromising a protective IED must be counted only once. To address this issue, a binary variable, $\varepsilon$, is defined for each of the components of each shared substation. to indicate (with a value equal to 1) that component (protective IED or feeder) is targeted by hybrid attackers in at least one of the minimal cut-sets. In response, (2a)-(2d) are defined.

$$\sum (\zeta^s_{c,p}.\mu^s_{c,p}) \le M.\varepsilon^s_p \quad \forall s \in \bar{S}, p \in \bar{I}_s \tag{2a}$$

$$\varepsilon^s_p \le \sum (\zeta^s_{c,p}.\mu^s_{c,p}) \quad \forall s \in \bar{S}, p \in \bar{I}_s \tag{2b}$$

$$\sum (\tau^s_{c,f}.\mu^s_{c,f}) \le M.\varepsilon^s_f \quad \forall s \in \bar{S}, f \in \bar{F}_s. \tag{2c}$$

$$\varepsilon^s_f \le \sum (\tau^s_{c,f}.\mu^s_{c,f}) \quad \forall s \in \bar{S}, f \in \bar{F}_s. \tag{2d}$$

When a component at a shared substation is targeted in at least one minimal cut-set (i.e., $\mu^s_{c,p}=1$ for IED $p$ in minimal cut-set $c$ of substation $s$ and $\mu^s_{c,f}=1$ for feeder $f$ in minimal cut-set $c$ of substation $s$) by hybrid attackers, it is flagged (i.e., $\varepsilon^s_p=1$ for IED $p$ at substation $s$ and $\varepsilon^s_f=1$ for feeder $f$ at substation $s$), and its corresponding resources (i.e., $\lambda^{cy}_{s,p}$ for IED $p$ at substation $s$ and $\lambda^{ph}_{s,f}$ for feeder $f$ at substation $s$) are considered only once. This is guaranteed by (2a)-(2d). Constraint (2a) and (2b) concern the protective IEDs at substation $s$, while constraint (2c) and (2d) are imposed on each of MV feeders of shared substation $s$. So as to flag targeted components for each component of a minimal cut-set of a shared substation, a set of constraints is introduced as follows:

$$\sum_{f \in \vec{\psi}^s_c} (\tau^s_{c,f}.\mu^s_{c,f}) + \sum_{p \in \vec{\psi}^s_c} (\zeta^s_{c,p}.\mu^s_{c,p}) \le M.\chi^s_c \quad \forall s \in \bar{S}, c \in \bar{C}_s \tag{3a}$$

$$\zeta^s_{c,p}.\chi^s_c \le \mu^s_{c,p} \quad \forall s \in \bar{S}, c \in \bar{C}_s, p \in \bar{I}_s \tag{3b}$$

$$\tau^s_{c,f}.\chi^s_c \le \mu^s_{c,f} \quad \forall s \in \bar{S}, c \in \bar{C}_s, \forall f \in \bar{F}_s \tag{3c}$$

$$\mu^s_{c,f} \le \tau^s_{c,f} \quad \forall s \in \bar{S}, c \in \bar{C}_s, \forall f \in \bar{F}_s \tag{3d}$$

$$\mu^s_{c,p} \le \zeta^s_{c,p} \quad \forall s \in \bar{S}, c \in \bar{C}_s, p \in \bar{I}_s \tag{3e}$$

In (3a), $\chi^s_c$ is used to flag the minimal cut-set $c$ at substation $s$ selected by the hybrid attackers. In this constraint, when a component of minimal cut-set $c$ is compromised by the attackers (i.e., $\mu^s_c=1$), the minimal cut-set is flagged. However, when hybrid attackers select a minimal cut-set (i.e., $\chi^s_c=1$), they have to compromise all of its components (i.e., $\mu^s_{c,p}=\mu^s_{c,f}=1$). This is enforced by (3b) for protective IEDs. Similarly, this is imposed on MV feeders to be faulted by (3c). However, the binary variable $\mu^s_{c,f}$ or $\mu^s_{c,p}$ can only take a value of one when MV feeder $f$ or protective IED $p$ is a member of minimal cut-set $c$ (i.e., $\zeta^s_{c,p}$ and $\tau^s_{c,f}$ are equal to 1). These requirements are ensured by (3d) and (3e), respectively.

In addition, a minimal cut-set of shared substation $s$ could directly de-energize the MV feeder $f$, and in such a case, the value of the binary variable $\varpi^s_f$ should be set to one. This is enforced by (4a) and (4b). Thus, the amount of load shedding of MV feeder $f$ would be equal to its load demand at the attack time, namely $P^{de}_{s,f}$. This is represented in (4c).

$$\sum_{=} (\chi^s_c.\sigma^s_{c,f}) \le M.\varpi^s_f \quad \forall s \in \bar{S}, f \in \bar{F}_s \tag{4a}$$

$$\varpi^s_f \le \sum_{=} (\chi^s_c.\sigma^s_{c,f}) \quad \forall s \in \bar{S}, f \in \bar{F}_s \tag{4b}$$

$$P^{fsh}_{s,f} = P^{de}_{s,f}.\varpi^s_f \quad \forall s \in \bar{S}, \forall f \in \bar{F}_s \tag{4c}$$

In (4a) and (4b), $\sigma^s_{c,f}$ represents whether MV feeder $f$ is directly de-energized in minimal cut-set $c$. To model the relationships between transmission lines and selected minimal cut-sets, (5a) and (5b) are incorporated into the model:

$$\sum \sum_{=} (\chi^s_c.h^s_{c,l}) \le \alpha_l.M \quad \forall l \in \bar{L} \tag{5a}$$

$$\alpha_l \le \sum \sum_{=} (\chi^s_c.h^s_{c,l}) \quad \forall l \in \bar{L}. \tag{5b}$$

In (5a) and (5b), $h^s_{c,l}$ represents whether minimal cut-set $c$ of substation $s$ leads to the de-energization of transmission line $l$. Based on these two constraints, a transmission line connected to a shared substation is de-energized (i.e., $\alpha_l=1$) if the substation is attacked in a way that triggers the protection system of line $l$, which is given in (5a). In addition, a transmission line is de-energized due to the hybrid attacks if at least one of the minimal cut-sets leading to its de-energization is selected by hybrid attackers. In this regard, constraint (5b) is imposed on each transmission line. Now, based on the defined variables and parameters, the resource constraints are formulated as follows:

$$\sum \sum_{=} (\varepsilon^s_f.\lambda^{ph}_{s,f}) \le AR_{ph} \tag{6a}$$

$$\sum_{s}\sum_{p}(\varepsilon_{p}^{s}.\lambda_{s,p}^{cy}) \le AR_{cy}. \quad (6b)$$

These two constraints imply that the coordinated hybrid attacks against shared substations are feasible only if the required resources are kept within the budget. Constraint (6a) represents the resources required to create man-made faults on MV feeders. Additionally, constraint (6b) imposes a limitation on the resources required for launching cyber-attacks against IEDs. The attacker's total resource budget (i.e., $AR_{ph}$ for causing man-made faults and $AR_{cy}$ for launching cyber-attacks against IEDs) is set to predefined levels. Due to the unavailability of such information. Thus, the selected budget values are based on the commonly adopted assumptions in the related literature [25]. In addition, the resources required for changing protection settings of protective device $p$ ( $\lambda_{s,p}^{cy}$) and causing man-made faults on MV feeder $f$ at shared substation $s$ ( $\lambda_{s,f}^{ph}$) are considered as the attackers' constraints. In doing so, varying levels of difficulty in launching attacks on different components are taken into account.

### C. Lower-Level Problem

After the occurrence of the coordinated hybrid attacks, the TSO responds by controlling the power output of generation units and the amount of load shedding at different nodes. Nevertheless, the TSO's response to the hybrid attacks is subject to a set of constraints, which are as follows:

$$[B]\underline{\delta} = P^{gen} - P^{load} + P^{sh} + P^{fsh} \quad (7)$$

$$P_g^{gen,\min} \le P_g^{gen} \le P_g^{gen,\max} \quad \forall g \in \bar{G} \quad (8a)$$

$$P_g^{gen} = P_g^{gen0} + \Delta_g^u - \Delta_g^l \quad \forall g \in \bar{G} \quad (8b)$$

$$0 \le \Delta_g^u, \Delta_g^l \quad \forall g \in \bar{G} \quad (8c)$$

$$-(1-\alpha_l).\mathrm{T}_l^{line,\max} \le \mathrm{T}_l^{line} \le (1-\alpha_l).\mathrm{T}_l^{line,\max} \quad \forall l \in \bar{L} \quad (9)$$

$$-\alpha_l.M \le \mathrm{T}_l^{line} - \frac{\delta_i - \delta_j}{x_{l,i-j}} \le \alpha_l.M \quad \forall l \in \bar{L} \quad (10)$$

$$0 \le P_i^{sh} \le P_i^{load} \quad \forall i \in \bar{N} \setminus \bar{S} \quad (11a)$$

$$0 \le P_i^{sh} + \sum_{f \in \bar{F}_i} P_{i,f}^{fsh} \le P_i^{load} \quad \forall i \in \bar{S} \quad (11b)$$

$$-\pi \le \delta_i \le \pi \quad \forall i \in \bar{N}, i \ne 1 \quad (12a)$$

$$\delta_1 = 0. \quad (12b)$$

Constraint (7) stands for the compact form of power balance at nodes of a TS. The upper and lower generation limits (i.e., $P_g^{gen,\max}$ and $P_g^{gen,\min}$) are imposed by (8a) on generation units. In addition, two non-negative continuous variables are defined for each generation unit to measure the changes in their power output compared to the pre-attack power output ( $\Delta_g^u$ for upward changes and $\Delta_g^l$ for downward changes). In this sense, constraint (8b) is imposed on each generation unit. When a transmission line is de-energized by hybrid attackers (i.e., $\alpha_l = 1$), the flow on the line must be set to zero. This is enforced by constraint (9). The power flow on an energized transmission line ( $\mathrm{T}_l^{line}$) is limited by (9) as well.

In (10), the relationship between the power flow on a transmission line and its ending voltage angles (i.e., $\delta_i$ and $\delta_j$ ) is expressed. However, as this relationship must be applied to only energized lines, the big-M approach is deployed in this constraint. In doing so, for de-energized lines, this constraint is relaxed. Constraint (11a) limits the amount of load shedding at non-shared nodes. For shared-substation nodes, the load shedding can consist of two components: load shedding caused directly by the hybrid attacks ( $P_{i,f}^{fsh}$) and load shedding implemented by the TSO ( $P_i^{sh}$) to alleviate operational violations. This is expressed in (11b). Finally, constraints (12a) and (12b) specify the allowable variation of voltage angles.

## VI. Simulation Results

This section presents the test system under study along with the underlying assumptions. Subsequently, the proposed framework is implemented on the test system, and the results are analyzed and discussed.

### A. Simulation Setup

In this section, all simulations are deterministic. For each scenario, the optimization model is solved once, and the reported results correspond to that single solve.

#### 1- Modified Test System:

The case studies are conducted based on a modified version of the IEEE 24-bus reliability test system (RTS) [26]. The original system is modified as follows:

- In order to put more stress on transmission lines, the line capacities are multiplied by 0.8.
- Each shared substation has four MV feeders, and the load of each shared substation has been equally distributed among its four feeders. In addition, the total load for each feeder is modeled as a single aggregated point at the beginning of the MV feeder.

The modifications to this test system are reported in Table A.1 (in the Appendix), and the single-line diagram of this grid is shown in Fig. 6. In addition, the grid is operated according to the *N-1* criterion before hybrid attacks.

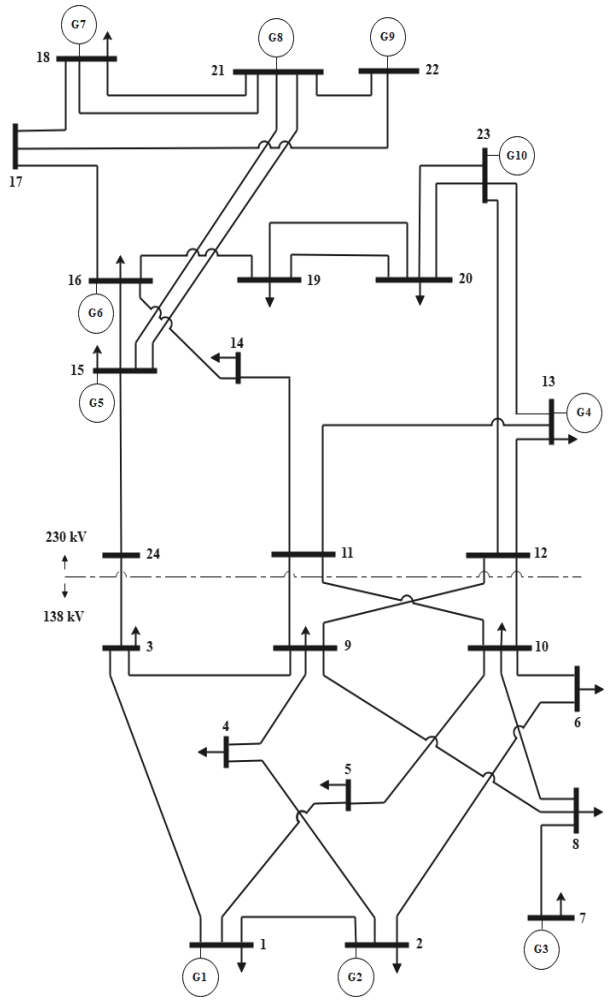


Fig. 6. IEEE reliability test system [26].

*2- Simulation Environment and Solver Details*

The proposed mixed integer bilevel optimization model is implemented in GAMS environment and is solved using JAMS. The JAMS solver was used with default settings, including the default optimality and feasibility tolerances, as follows:

- GAMS version: 49.6.1
- Solver: JAMS
- Absolute objective gap tolerance: **1e-10**
- Relative objective gap tolerance (optcr): **1e-4**
- Maximum constraint violation tolerance: **1e-8**

In addition, the bilevel problem is automatically reformulated by JAMS into a single-level MPEC using KKT optimality conditions.

*3- General Assumptions on Attack Resources*

It should be notified that the resources required to change the protection settings of the IEDs at each shared substation depend on the cybersecurity measures in the substations. As real-world data about such events are not publicly available, these data are assumed. The resources required for causing man-made faults on a distribution feeder are assumed to be 1 resource unit. In addition, the resources to be used for compromising an IED (feeder, transformer, …) are also assumed equal to 1 resource unit. For the sake of simplicity, these data are assumed to be the same for all the substations.

*4- The Shared Substation Configurations*

In the test system under study, it is assumed that nodes 3-6 and 8-10 represent the shared substations between the DSOs and the TSO. Indeed, they represent the substations at the interface between MV and HV grids.

In the simulations, two different protection configurations are considered, which are listed in Table I. For shared substations N9 and N10, an IEC 61850 based layout is considered. This layout is a combination of breaker-and-a-half and double breaker-double bus configurations. However, the protection layout of the other shared substations is double breaker-double bus in [27].

TABLE I
Configurations, Minimal Cutt-set Numbers, and Target Lines of the Shared Substations

| Substation # | Configuration | Minimal Cut-set Number | Target Lines | #Target Lines |
|---|---|---|---|---|
| **3** | Double breaker-double bus | 24 | 3-24, 3-9, 3-1 | 3 |
| **4** | Double breaker-double bus | 16 | 4-9, 4-2 | 2 |
| **5** | Double breaker-double bus | 16 | 5-1, 5-10 | 2 |
| **6** | Double breaker-double bus | 16 | 6-2, 6-10 | 2 |
| **8** | Double breaker-double bus | 24 | 8-7, 8-9, 8-10 | 3 |
| **9** | IEC 61850 based | 28 | 9-3, 9-4, 9-8, 9-11, 9-12 | 5 |
| **10** | IEC 61850 based | 28 | 10-1, 10-6, 10-8, 10-11, 10-12 | 5 |

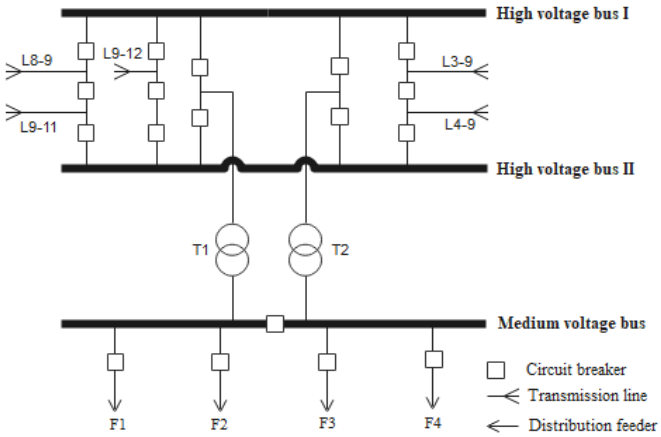


Fig. 7. Layout of shared substation N9 (IEC 61850 based), including breaker-and-a-half and double-breaker-double-bus configurations [13], [27].

The protection scheme of N9 is depicted in Fig. 7. The high-voltage bus and medium-voltage bus are connected through the step-down transformers, namely T1 and T2. We notice that the high-voltage section of this substation includes both breaker-and-a-half and double-bus-double-breaker configurations. The

description of the high-voltage section along with the two transformers is given in Table II. In normal conditions, all CBs are closed. For the configuration of the substation shown in Fig. 7, 28 minimal cut-sets are deduced. All derived minimal cut-sets for the shared substation N9 are reported in Table A.2 of the Appendix. Accordingly, the matrices introduced in the Appendix are constructed. Similar procedure is done for the other substations.

TABLE II
Description of High-Voltage Section of the Substation N9

| Equipment | Numbers in Use |
|---|---|
| **High-Voltage Bus** | 2 |
| **Transmission Line Bay** | 5 |
| **Transformer Bay** | 2 |
| **Protective IEDs** | 9 |

## B. Results

***Case study I***: *Base Case*

In the base case simulations, the budget for launching the cyber-attack ( $AR_{cy}$) is limited to 18, and the attackers' total budget for creating man-made faults on MV feeders ( $AR_{ph}$) is equal to 3. Without loss of generality, the resources required for causing man-made faults on an MV feeder ( $\lambda_{s,f}^{ph}$) are assumed to be 1 resource unit. In addition, the resources to be used for compromising an IED ( $\lambda_{s,p}^{cy}$) are also assumed equal to 1 resource unit. In this case study, the value of $\beta$ in the lower-level objective function is set to 0.001. These input parameters as well as the results of this analysis are reported in Table III.

TABLE III
Input Parameters and Corresponding Simulation Results in Case Study I for the Given Budget Pair

| **Input Parameters and Values** | | | |
|---|---|---|---|
| **$AR_{ph}$** | $AR_{cy}$ | $\lambda_{s,f}^{ph}, \lambda_{s,p}^{cy}$ | β |
| **3** | 18 | 1 | 0.001 |
| **Results** | | | |
| **Selected Cut-sets** | Configuration | Cut-set Components | De-energized Lines |
| **N3.c1** | Double breaker-double bus | F1, T1, BI, L1-3 | 1-3 |
| **N3.c9** | Double breaker-double bus | F1, T1, BI, L3-24 | 3-24 |
| **N9.c7** | IEC 61850 based | F3, T2, BII, L9-11 | 9-11 |
| **N9.c11** | IEC 61850 based | F3, T2, BI, L9-12 | 9-12 |
| **N9.c19** | IEC 61850 based | F3, T2, BII, L4-9 | 4-9 |
| **N10.c6** | IEC 61850 based | F4, T2, BII, L8-10 | 8-10 |
| **N10.c12** | IEC 61850 based | F4, T2, BII, L5-10, L6-10 | 5-10, 6-10 |
| **Direct Shedding** | Indirect Shedding | Targeted Substations | |
| **278 MW** | 309 MW | N3, N9, N10 | |

The minimal cut-sets selected by the attackers to maximize their objective are also shown in Table III. In this table, N3.c1 refers to cut-set 1 of shared substation N3. In addition, 'BI' represents the high voltage bus I of substations, as depicted in Fig. 7. Seven minimal cut-sets are selected by the attackers, and these lead to de-energization of eight transmission lines. As a consequence, the 138 kV area is almost disconnected from the 230 kV area in the grid under study (See Fig. 6). In addition, except for the load at N10, the generation units located in the 230 kV area cannot contribute to supplying the loads in 138 kV area, and the generation capacity of this area is insufficient to meet the remaining demand. Specially, the generation units connected to nodes N1 and N2 reach the maximum capacity limits. Nonetheless, due to the capacity of line 7-8, the generation connected to node N7 cannot be operated at its maximum capacity. Although 278 MW of load has already been disconnected from the grid due to direct load shedding, the TSO has to curtail some load due to generation shortages as well as transmission congestion in the 138 kV area. Thus, the TSO responds to the cyber-attacks by rescheduling the generation units. The amount of indirect load shedding in this case is 309 MW, which exceeds the amount of the direct load shedding. As shown in Table III, the shared substations N3, N9, and N10 are targeted by hybrid attackers in this case, as they are among those that connect the 230 kV area to the 138 kV area. In doing so, the hybrid attackers not only cause load shedding but also weaken the connections between 138 kV and 230 kV areas. Based on the protection configurations of shared substations N3, N9 and N10, there are 24, 28 and 28 candidate minimal cut-sets for these three substations, respectively. In this case study, the model's execution time is 15.41 *s*. In addition, the model consists of 3499 equations and 1762 variables.

***Case study II***: *Sensitivity analysis with respect to attackers' resources*

In order to study the impact of attacker's budget on the results, a sensitivity analysis is conducted. To do so, eight different scenarios are defined, as shown in Table IV. All other conditions are the same as those in Case study I.

TABLE IV
Different Scenarios for Attackers' Total Budgets

| **Scenario #** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
|---|---|---|---|---|---|---|---|---|
| **$AR_{ph}$** | 1 | 1 | 2 | 3 | 3 | 3 | 4 | 5 |
| **$AR_{cy}$** | 2 | 5 | 8 | 10 | 13 | 18 | 18 | 18 |

The results in terms of direct, indirect, and total load shedding are shown in Fig. 8. As the attackers' budgets increase, the amount of total load shedding also increases. However, the direct and indirect load shedding follow different patterns. For budget scenarios 1-5, the amount of direct load shedding is greater than that of indirect load shedding. In contrast, indirect load shedding exceeds direct load shedding for scenarios 6-8. The justification for this observation is that the hybrid attackers are able to weaken the connection between the two areas or even disconnect the 138 kV area from the other area in scenarios 6-8. By doing so, the power grid is split into two areas. While the generation capacity of the 230 kV area is

more than its load demand, the 138 kV area suffers a generation shortage. Therefore, the TSO has to implement load-shedding program. In scenarios 7 and 8, the two areas are totally disconnected from each other. In addition, line 7-8 becomes overloaded in some scenarios. For example, in budget scenario 3, the attackers target transmission lines 8-9 and 8-10 via the hybrid-attacks. This leads to a direct load shedding of 185 MW. In this situation, node N8 is connected to only N7 through line 7-8. Nonetheless, the capacity of line 7-8 is lower than the load demand at node N8, and it becomes overloaded after the attacks. In response, TSO curtails 31 MW of load at node N8 to bring the power flow on this line within the limits.

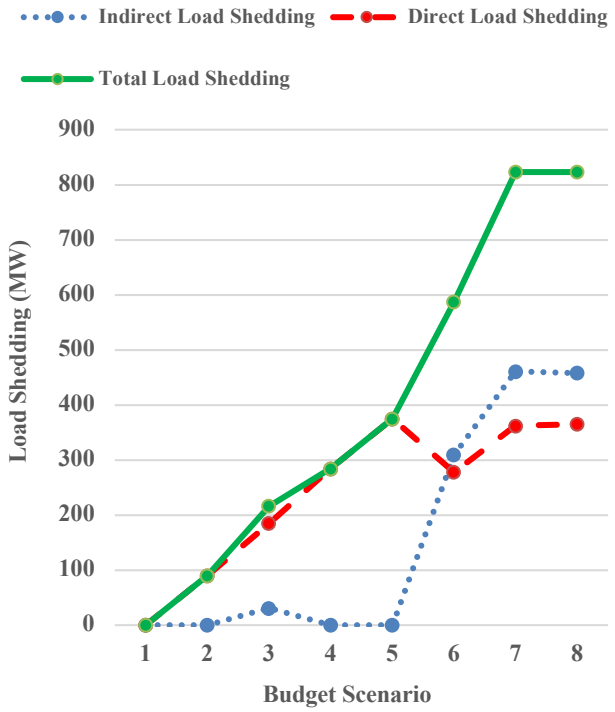


Fig. 8. Amounts of direct, indirect, and total load shedding caused by the hybrid attacks for different budget scenarios.

Furthermore, the results in terms of the number of transmission-line outages are shown in Fig. 9. For budget scenario 1, the available resources for manipulating IEDs are not enough to target the grid via a minimal cut-set. In addition, in order to see the impacts of different $AR_{cy}$ on the results, a comparison between scenarios 4 and 5 is made. These two budget scenarios are similar in terms of the resources required to create man-made faults. Nonetheless, scenario 5 causes four line outages, while scenario 4 leads to two line outages. The reason for this is that five minimal-cut-sets are selected by the attackers under budget scenario 5. Another comparison can be made for scenarios 6 and 7. These two scenarios have the same $AR_{cy}$. When scenarios 6 and 7 are compared, it is found out that they respectively lead to 8 and 6 transmission line outages. However, the attackers are able to select 5 minimal cut-sets in scenario 7, thereby resulting in a total load shedding of 823 MW. This load shedding exceeds that of scenario 6 by 236 MW. It is worth mentioning that the main objective of cyber attackers is to cause load shedding. Thus, the attacks are launched in a way that cause the maximum amount of load shedding in each situation.

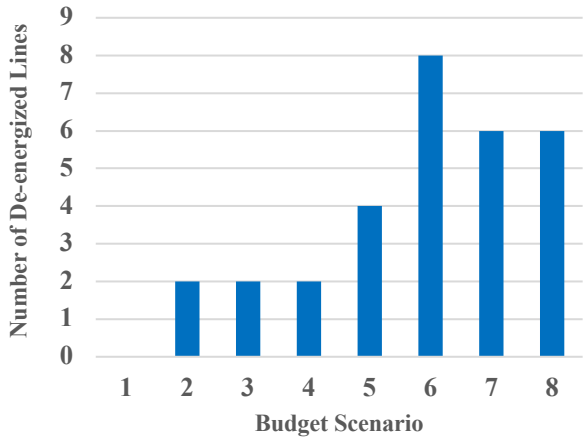


Fig. 9. Number of transmission lines de-energized owing to the hybrid attacks for different budget scenarios.

***Case study III***: *Impact of generation availability*

In order to study the impact of unavailability of generation units on the results, four different operational conditions are considered. In conditions 2-4, it is assumed that a generation unit is unavailable due to scheduled maintenance or forced outages. As can be seen in Fig. 6, the test system is divided into two main areas: 138 kV and 230 kV areas. The generation units are mainly in the 230 kV area. Consequently, the capacity of generation units in the 138 kV area is less than the load demand in normal conditions. Thus, the generation deficit is imported from the 230 kV area through interconnection lines. In this regard, as discussed earlier, the attackers would target the interconnection lines. The conditions are the results are summarized in Table V. However, all other assumptions are the same as Case Study I.

TABLE V
Input Data and Results for Case Study III

| **Condition #** | **Condition 1** | **Condition 2** | **Condition 3** | **Condition 4** |
|---|---|---|---|---|
| - | All Units In | G1 Out | G3 Out | G5 Out |
| **Capacity and Location Area of Unavailable Units** | | | | |
| **Unit** | | G1 | G3 | G5 |
| **Capacity** | | 192 MW | 300 MW | 215 MW |
| **Location Area** | | 138 kV | 138 kV | 230 kV |
| **Results** | | | | |
| **Direct Shedding** | 278 MW | 275 MW | 256 MW | 278 MW |
| **Indirect Shedding** | 309 MW | 514 MW | 478 MW | 309 MW |
| **Total Shedding** | 587 MW | 789 MW | 734 MW | 587 MW |
| **Overloaded Lines** | 7-8 | 7-8, 8-10 | - | 7-8 |

In condition 1, all generation units are available. This condition was analyzed in detain in Case Study I. However,

unavailability of unit G1 significantly worsens the amount of load shedding. As can be traced in Table V, the hybrid-attacks increase the total load shedding from 587 MW to 789 MW. In this condition, the attackers target almost all interconnection lines between the two areas. As a consequence, the lower area (138 kV) cannot import its power deficit from the upper area (230 kV). Additionally, two transmission lines 7-8 and 8-10 are overloaded, and the TSO has to bring them back to their allowable limits through implementing load-shedding programs. This leads to additional load shedding in the 138 kV area. The same analysis can be performed for generation unit 3.

Due to the big surplus of generation capacity (2721 MW) in the upper area compared to the area's total load (1518 MW) and high capacities of its transmission lines, the unavailability of a unit in 230 kV area results in limited or no change in the results as we as attackers' strategy. This can be observed in Condition 4, in which the results are the same as Condition 1. With this in mind, for this test system, if the hybrid attacks are launched during the unavailability of the 138-kV-located generation units, they can be more impactful.

## VII. Conclusions and Future Research

This paper raised concerns about the cybersecurity of shared substations. A new attack vector from MV to HV grids was introduced and analyzed. The main insights derived from this case-study-based modeling analysis are as follows:

- The analysis indicates that cross-domain threats in shared substations may represent a relevant cybersecurity concern.
- The results further suggest that limited consideration of cross-domain threat propagation, along with the significant impacts of these incidents, could represent a vulnerability area.
- This study provides an impact-assessment modeling tool that may inform discussions between TSOs and DSOs on enhancing cyber-physical security practices and managing cross-domain risks in shared infrastructures**.**
- The quantitative magnitude of the impacts of the attacks is case-study dependent and may vary depending on system topology, protection configurations, attack resources, and operational settings.

The proposed framework may also inform discussions among regulators and system operators, for example, by helping to identify critical processes, involved entities (e.g., DSOs and TSOs), and associated assets (e.g., IEDs). TSOs typically categorize processes, assets, and entities using high- and critical-impact thresholds, which are determined by quantifying potential load shedding under various cyber-attacks. This methodology bridges detailed substation protection logic and system-level impact assessment. Thus, it can enable the evaluation of cyber-physical threats originating at distribution levels. In this regard, this framework may help TSOs do this task, including threats from a DSO's domain to the TSO's domain.

Despite the contributions of this framework, certain limitations should be acknowledged. Future research could address these areas:

- No probabilistic defense or mitigation layer is modelled.
- The model assumes successful manipulation of protection IEDs and fault initiation without considering detection or operator intervention.
- Attacker resources and costs are assumption-driven rather than empirically calibrated.
- Dynamic phenomena such as communication delays, protection timing, or operator response are not explicitly modeled.
- The results are derived from a modified IEEE 24-bus test system, which may not fully capture the complexity of real large-scale power systems. In addition, the model adopts an equal load split assumption for MV feeders. This is explicitly treated as a stylized input rather than a realistic representation of all operational configurations.
- The identification of minimal paths is performed manually. However, this is not the focus of the present work.

## Acknowledgment

The authors would like to express their gratitude to Dr. Efthymios Karangelos and Dr. Mevludin Glavic for their insightful comments and helpful feedback, which improved the quality of this paper.

## Appendix

### A. Matrix Representation of Minimal Cut-sets

In this part, the minimal cut-set approach is expressed in the form of several matrices. In doing so, the approach is formulated in a general and systematic way. To this end, three matrices are introduced, namely the minimal-cut-set ( $\Psi$ ), target-line ( $H$ ), and target-feeder matrices ( $\Delta$ ). In addition, in order to distinguish between MV feeders and protective IEDs, $\Psi$ is split into two submatrices: $\Gamma$ (man-made fault matrix) and $Z$ (compromised-IED matrix). These matrices serve as inputs to the bilevel optimization problem. These matrices are constructed for each shared substation as well. Moreover, they can be constructed for any configurations of substations.

However, for illustrative purposes, these matrices are introduced and constructed for Fig. 3, as follows:

$$\left[\Psi_s\right]_{10\times4} = \begin{bmatrix} \tilde{\psi}^s_{c=1} \\ \tilde{\psi}^s_{c=2} \\ \tilde{\psi}^s_{c=3} \\ \tilde{\psi}^s_{c=4} \end{bmatrix}_{10\times4} = \left[\left[\Gamma_s\right]_{4\times4};\left[Z_s\right]_{6\times4}\right]_{10\times4} \qquad \text{(A.1a)}$$

The matrix corresponding to the dotted black block in Fig. 3 is formed as:

$$\Gamma_s = \begin{bmatrix} \tau^s_{1,f1} & \tau^s_{1,f2} & \tau^s_{1,f3} & \tau^s_{1,f4} \\ \tau^s_{2,f1} & \tau^s_{2,f2} & \tau^s_{2,f3} & \tau^s_{2,f4} \\ \tau^s_{3,f1} & \tau^s_{3,f2} & \tau^s_{3,f3} & \tau^s_{3,f4} \\ \tau^s_{4,f1} & \tau^s_{4,f2} & \tau^s_{4,f3} & \tau^s_{4,f4} \end{bmatrix} = \begin{bmatrix} \overset{F1}{1} & \overset{F2}{0} & \overset{F3}{0} & \overset{F4}{0} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{(A.1b)}$$

The matrix corresponding to the dashed blue block in Fig. 3 is constructed as:

$$Z_s = \begin{bmatrix} \zeta^s_{1,f1} & \zeta^s_{1,f2} & \zeta^s_{1,f3} & \zeta^s_{1,f4} & \zeta^s_{1,T1} & \zeta^s_{1,T2} \\ \zeta^s_{2,f1} & \zeta^s_{2,f2} & \zeta^s_{2,f3} & \zeta^s_{2,f4} & \zeta^s_{2,T1} & \zeta^s_{2,T2} \\ \zeta^s_{3,f1} & \zeta^s_{3,f2} & \zeta^s_{3,f3} & \zeta^s_{3,f4} & \zeta^s_{3,T1} & \zeta^s_{3,T2} \\ \zeta^s_{4,f1} & \zeta^s_{4,f2} & \zeta^s_{4,f3} & \zeta^s_{4,f4} & \zeta^s_{4,T1} & \zeta^s_{4,T2} \end{bmatrix} = \quad \text{(A.1c)}$$

$$\begin{bmatrix} \overset{F1}{1} & \overset{F2}{0} & \overset{F3}{0} & \overset{F4}{0} & \overset{T1}{1} & \overset{T2}{0} \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

The matrix corresponding to the solid green block in Fig. 3 is formed as:

$$H_s = \begin{bmatrix} \tilde{h}^s_{c=1} \\ \tilde{h}^s_{c=2} \\ \tilde{h}^s_{c=3} \\ \tilde{h}^s_{c=4} \end{bmatrix} = \begin{bmatrix} h^s_{1,L1} & h^s_{1,L2} \\ h^s_{2,L1} & h^s_{2,L2} \\ h^s_{3,L1} & h^s_{3,L2} \\ h^s_{4,L1} & h^s_{4,L2} \end{bmatrix} = \begin{bmatrix} \overset{L1}{1} & \overset{L2}{0} \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{(A.1d)}$$

The matrix corresponding to the solid orange block in Fig. 3 is constructed as:

$$\Delta_s = \begin{bmatrix} \sigma^s_{1,f1} & \sigma^s_{1,f2} & \sigma^s_{1,f3} & \sigma^s_{1,f4} \\ \sigma^s_{2,f1} & \sigma^s_{2,f2} & \sigma^s_{2,f3} & \sigma^s_{2,f4} \\ \sigma^s_{3,f1} & \sigma^s_{3,f2} & \sigma^s_{3,f3} & \sigma^s_{3,f4} \\ \sigma^s_{4,f1} & \sigma^s_{4,f2} & \sigma^s_{4,f3} & \sigma^s_{4,f4} \end{bmatrix} = \begin{bmatrix} \overset{F1}{1} & \overset{F2}{1} & \overset{F3}{0} & \overset{F4}{0} \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad \text{(A.1e)}$$

In (A.1a), $\Psi_s$ is a matrix that represents the components of all minimal cut-sets at shared substation *s*. However, $\tilde{\psi}^s_c$ is a vector that stands for the component of minimal cut-set *c* at substation *s*. We partition $\Psi_s$ into two submatrices, namely $\Gamma_s$ and $Z_s$. The former corresponds to man-made faults on MV feeders. The latter, however, represents the compromised IEDs in each minimal cut-set. Therefore, it is related to cyber-attacks against IEDs.

In $\Gamma_s$, $\tau^s_{c,f}$ represents whether MV feeder *f*, in minimal cut-set *c*, and shared substation *s* has been made faulty by hybrid attackers. Similarly, $\zeta^s_{c,p}$ stands for whether protective IED *p* is compromised at shared substation *s* and minimal cut-set *c*. To identify which transmission lines are affected by a minimal cut-set, $H_s$ is constructed for each shared substation. This matrix links the minimal cut-sets to the transmission lines connected to the substation. In other words, if minimal cut-set *c* of substation *s* leads to the de-energization of transmission line *L*, $h^s_{c,L}$ is equal to 1, and zero otherwise. In addition, $\Delta_s$ is introduced to determine which MV feeders of an attacked shared substation are directly de-energized. The element of this matrix, $\sigma^s_{c,f}$, represents whether MV feeder *f* is directly de-energized because of hybrid attacks through minimal cut-set *c* of shared substation *s* or not.

### *B. A Complete Version of the GAMS Implementation*

**Scalars**

**pi, ARph Attackers' total budget for causing man-made faults, RScy Attackers' total budget for lunching cyber attacks;**

**sets**

**n Nodes, ds(n) Shared substations, g Generator units, l Transmission lines, ng(n,g) Nodes of generators, k Buse type, c Minima cut-sets, f MV feeders, pr Protection IEDs at shared substations;**

**Table bustype(n,k) Bus type Shared or normal (non-shared);**

**Table T(ds,c,f) Man-made faulted feeders;**

**Table Z(ds,c,pr) Compromised IEDs;**

**Table H(ds,c,l) De-energized transmission lines;**

**Table Delt(ds,c,f) De-energized MV feeders;**

**Table Landaf(ds,f) Resources required for causing man-made faults;**

**Table Landap(ds,pr) Resources required for compromising IEDs;**

**Table DF(ds,f) Load demand of shared substations;**

**parameters**

**Pg0(g) Initial generation of generation units before the cyber-attacks, ming(g) Lower generation limits, maxg(g) Upper generation limits, d(n) Bus load data,**

**x(l) Transmission line reactance,**

**ci(l,n) Incidence matrix for buses and transmission lines**

**fl(l) Transmission line capacities**

**gs(g) Generator state, b(l) susceptance.**

**b(l)=1/x(l);**

**variables**

**objin Lower-level objective function (LL)**

**objout Upper-level objective function (UL)**

**pfl(l) Power flow on transmission lines**

**delta(n) Voltage angle of each node in radians;**

**binary variables**

**alpha(l) Whether or not a transmission line is impacted due to the attacks**

**miu1(ds,c,pr) Whether or not a protective IED at a shared substation is compromised**

**miu2(ds,c,f) Whether or not an MV feeder at a shared substation is attacked**

**xi(ds,c) Whether or not minimal cut-set c is selected by attackers**

```
eps1(ds,pr) A binary variable representing whether or not a protection IED is compromised at a shared substation
eps2(ds,f) Whether or not an MV feeder at a shared substation is compromised
omeg(ds,f) Whether or not an MV feeder is de-energized as a result of a cyber attack;
positive variables
lcv(n) Indirect load curtailment due to constraint violations
lca(n) Direct load curtailment due to the attacks
p(g) Power output of generation units
deltu(g) The increase in power output of unit g compared to its original power output before the attacks
deltl(g) The decrease in power output of unit g compared to its original power output before attacks;
equations
defout .. objout=e=sum(n,lcv(n)+lca(n));
defin .. objin=e=(sum(n,lcv(n)))+(0.001*sum(g,deltu(g)+deltl(g)));
eq1(g).. p(g)=g=ming(g);
eq2(g).. p(g)=l=maxg(g);
eq3(l).. pfl(l)=g=-fl(l)*(1-alpha(l));
eq4(l).. pfl(l)=l=fl(l)*(1-alpha(l));
eq5(n).. sum(l, pfl(l)*ci(l,n))+(sum(g$ng(n,g),p(g)*gs(g))-d(n)+lca(n)+lcv(n))=e=0;
eq6(l).. sum(n, b(l)*ci(l,n)*delta(n))*100+pfl(l)=g=-1000*(alpha(l));
eq7(l).. sum(n, b(l)*ci(l,n)*delta(n))*100+pfl(l)=l=1000*(alpha(l));
eq8(n).. delta(n)=g=-pi;
eq9(n).. delta(n)=l=pi;
eq10.. delta('n1') =e= 0;
eq11(n).. lca(n)+lcv(n)=l=d(n);
eq12(n)$(bustype(n,'normal')=1).. lca(n)=e=0;
eq13(ds,pr).. sum(c,Z(ds,c,pr)*miu1(ds,c,pr))=l=30*eps1(ds,pr);
eq14(ds,f).. sum(c,T(ds,c,f)*miu2(ds,c,f))=l=30*eps2(ds,f);
eq15(ds,c,f).. miu2(ds,c,f)=l=T(ds,c,f);
eq16(ds,c,pr).. miu1(ds,c,pr)=l=Z(ds,c,pr);
eq17(ds,c).. sum(f,miu2(ds,c,f))=l=20*xi(ds,c);
eq18(ds,c).. sum(pr,miu1(ds,c,pr))=l=20*xi(ds,c);
eq19(ds,c,pr).. (Z(ds,c,pr)*xi(ds,c))=l=miu1(ds,c,pr);
eq20(ds,c,f).. (T(ds,c,f)*xi(ds,c))=l=miu2(ds,c,f);
eq21(l).. sum(ds,sum(c,xi(ds,c)*H(ds,c,l)))=l=50*alpha(l);
eq22(l).. alpha(l)=l= sum(ds,sum(c,xi(ds,c)*H(ds,c,l)));
eq23.. sum(ds,sum(f,eps2(ds,f)*Landaf(ds,f)))=l=ARph;
eq24.. sum(ds,sum(pr,eps1(ds,pr)*Landap(ds,pr)))=l=ARcy;
eq25(ds,f).. sum(c,xi(ds,c)*Delt(ds,c,f))=l=20*omeg(ds,f);
eq26(ds,f).. omeg(ds,f)=l=sum(c,xi(ds,c)*Delt(ds,c,f));
eq27(ds).. lca(ds)=e=sum(f,DF(ds,f)*omeg(ds,f));
eq28(g).. p(g)=e=Pg0(g)+deltu(g)-deltl(g);
eq29(ds,pr).. eps1(ds,pr)=l=sum(c,Z(ds,c,pr)*miu1(ds,c,pr));
eq30(ds,f).. eps2(ds,f)=l= sum(c,T(ds,c,f)*miu2(ds,c,f));
option solver=jams;
Model bard / all /;
$echo bilevel alpha lca miu1 miu2 xi omeg min objin p pfl delta lcv deltu deltl defin eq1 eq2 eq3 eq4 eq5 eq6 eq7 eq8 eq9 eq10 eq11 eq28> "%emp.info%"
solve bard use emp max objout;
```

## C. *Extra Tables and Figures*

TABLE A.1
Some Important Data and the Modifications to the IEEE Reliability Test System

| Transmission Line Data | | | | | |
|---|---|---|---|---|---|
| Line # | Modified Capacity (MW) | Line # | Modified Capacity (MW) | Line # | Modified Capacity (MW) |
| 1-2 | 140 | 9-11 | 320 | 15-24 | 400 |
| 1-3 | 140 | 9-12 | 320 | 16-17 | 400 |
| 1-5 | 140 | 10-11 | 320 | 16-19 | 400 |
| 2-4 | 140 | 10-12 | 320 | 17-18 | 400 |
| 2-6 | 140 | 11-13 | 400 | 17-22 | 400 |
| 3-9 | 140 | 11-14 | 400 | 18-21 | 400 |
| 3-24 | 320 | 12-13 | 400 | 18-21 | 400 |
| 4-9 | 140 | 12-23 | 400 | 19-20 | 400 |
| 5-10 | 140 | 13-23 | 400 | 19-20 | 400 |
| 6-10 | 140 | 14-16 | 400 | 20-23 | 400 |
| 7-8 | 140 | 15-16 | 400 | 20-23 | 400 |
| 8-9 | 140 | 15-21 | 400 | 21-22 | 400 |
| 8-10 | 140 | 15-21 | 400 | - | - |
| Load Data | | | | | |
| Bus # | Load (MW) | Bus # | Load (MW) | Bus # | Load (MW) |
| 1 | 108 | 7 | 125 | 15 | 317 |
| 2 | 97 | 8 | 171 | 16 | 100 |
| 3 | 180 | 9 | 175 | 18 | 333 |
| 4 | 74 | 10 | 195 | 19 | 181 |
| 5 | 71 | 13 | 265 | 20 | 128 |
| 6 | 136 | 14 | 194 | - | - |
| Generation Unit Data | | | | | |
| Unit # | Generation Capability (MW) | Unit # | Generation Capability (MW) | Unit # | Generation Capability (MW) |
| G1 | 0-192 | G5 | 0-215 | G9 | 0-300 |
| G2 | 0-192 | G6 | 0-155 | G10 | 0-660 |
| G3 | 0-300 | G7 | 0-400 | - | - |
| G4 | 0-591 | G8 | 0-400 | - | - |
| Shared Substation Data | | | | | |
| Shared Substation # | Topology | Shared Substation # | Topology | Shared Substation # | Topology |
| 3 | DBDB* | 6 | DBDB | 10 | IEC |
| 4 | DBDB | 8 | DBDB | - | - |
| 5 | DBDB | 9 | IEC | - | - |

* Double breaker-double bus= DBDB
* IEC 61850 based= IEC

Each shared substation has 4 distribution feeders. In addition, for the sake of simplicity, it is assumed that the load of each shared substation is equally distributed among its four MV feeders.

TABLE A.2
The Components of All Minimal Cut-sets for the Shared Substation N9 (Shown in Fig. 7)

| Cut-set # | Components | De-energized Lines |
|---|---|---|
| C1 | F1, T1, BI, L8-9 | 8-9 |
| C2 | F2, T1, BI, L8-9 | 8-9 |
| C3 | F3, T2, BI, L8-9 | 8-9 |
| C4 | F4, T2, BI, L8-9 | 8-9 |
| C5 | F1, T1, BII, L9-11 | 9-11 |
| C6 | F2, T1, BII, L9-11 | 9-11 |
| C7 | F3, T2, BII, L9-11 | 9-11 |
| C8 | F4, T2, BII, L9-11 | 9-11 |
| C9 | F1, T1, BI, L9-12 | 9-12 |
| C10 | F2, T1, BI, L9-12 | 9-12 |
| C11 | F3, T2, BI, L9-12 | 9-12 |
| C12 | F4, T2, BI, L9-12 | 9-12 |
| C13 | F1, T1, BI, L3-9 | 3-9 |
| C14 | F2, T1, BI, L3-9 | 3-9 |
| C15 | F3, T2, BI, L3-9 | 3-9 |
| C16 | F4, T2, BI, L3-9 | 3-9 |
| C17 | F1, T1, BII, L4-9 | 4-9 |
| C18 | F2, T1, BII, L4-9 | 4-9 |
| C19 | F3, T2, BII, L4-9 | 4-9 |
| C20 | F4, T2, BII, L4-9 | 4-9 |
| C21 | F1, T1, BI, L8-9, L9-11 | 8-9, 9-11 |
| C22 | F2, T1, BI, L8-9, L9-11 | 8-9, 9-11 |
| C23 | F3, T2, BII, L8-9, L9-11 | 8-9, 9-11 |
| C24 | F4, T2, BII, L8-9, L9-11 | 8-9, 9-11 |
| C25 | F1, T1, BI, L3-9, L4-9 | 3-9, 4-9 |
| C26 | F2, T1, BI, L3-9, L4-9 | 3-9, 4-9 |
| C27 | F3, T2, BII, L3-9, L4-9 | 3-9, 4-9 |
| C28 | F4, T2, BII, L3-9, L4-9 | 3-9, 4-9 |

## REFERENCES


[1] Interaction Between Transmission and Distribution System Operators and an Assessment of Their Cooperation in Smart Grids," ISGAN Discussion Paper, 2014. [Online]. Available: https://www.iea-isgan.org/wp-content/uploads/2014/02/ISGAN_DiscussionPaper_TSODSOInteraction Overview_2014.pdf.

[2] S. Hussain, J. Hernandez Fernandez, A. K. Al-Ali, and A. Shikfa, ‘‘Vulnerabilities and countermeasures in electrical substations,’’ Int. J. Crit. Infrastruct. Protection, vol. 33, Jun. 2021.

[3] Electricity Information Sharing and Analysis Center, “Analysis of the cyber attack on the Ukrainian power grid,” 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC. Accessed on: Aug. 11, 2019.

[4] Network Code on Cybersecurity. [Online]. Available: https://www.entsoe.eu/network_codes/nccs/.

[5] M. Bahrami and L. Wehenkel, "Coordinated EV Charging Attacks to Cause Transmission Line Overloads," *2024 9th International Youth Conference on Energy (IYCE)*, Colmar, France, 2024, pp. 1-6.

[6] Y. Dvorkin and S. Garg, "IoT-enabled distributed cyber-attacks on transmission and distribution grids," *2017 North American Power Symposium (NAPS)*, Morgantown, WV, USA, 2017, pp. 1-6.

[7] M. P. Goodridge, S. Lakshminarayana and A. Zocca, "Uncovering Load-Altering Attacks Against N−1 Secure Power Grids: A Rare-Event Sampling Approach," in *IEEE Trans. Power Syst.*, doi: 10.1109/TPWRS.2024.3419725.

[8] S. Lakshminarayana, S. Adhikari and C. Maple, "Analysis of IoT-Based Load Altering Attacks Against Power Grids Using the Theory of Second-Order Dynamical Systems," in *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4415-4425, Sept. 2021, doi: 10.1109/TSG.2021.3070313.

[9] I. Zografopoulos et al., “Security assessment and impact analysis of cyberattacks in integrated T&D power systems,” in Proc. 9th Workshop Model. Simul. Cyber-Phys. Energy Syst., 2021, pp. 1–7.

[10] C. Qin, C Zhong, B. Sun, XL Jin, and Y. Zeng, “A tri-level optimal defense method against coordinated cyber-physical attacks considering full substation topology,” Appl. Energy, vol. 339, pp. 120961, Jun. 2023.

[11] K. Lai, M. Illindala, and K. Subramaniam, “A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment,” Appl. Energy, vol. 235, pp. 204–218, Feb. 2019.

[12] A. Apostolov and B. Vandiver, "IEC 61850 GOOSE applications to distribution protection schemes," *2011 64th Annual Conference for Protective Relay Engineers*, College Station, TX, USA, 2011, pp. 178-184, doi: 10.1109/CPRE.2011.6035618.

[13] Teng-Fa Tsao and Hong-Chan Chang, "Composite reliability evaluation model for different types of distribution systems," in *IEEE Trans. Power Syst.*, vol. 18, no. 2, pp. 924-930, May 2003, doi: 10.1109/TPWRS.2003.811174.

[14] Y. Liu, H. Gao, W. Gao and F. Peng, "Development of a Substation-Area Backup Protective Relay for Smart Substation," in *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2544-2553, Nov. 2017, doi: 10.1109/TSG.2016.2527687.

[15] H. C. Kiliçkiran, ˙Ibrahim ¸Sengör, H. Akdemir, B. Kekezo ˘glu, O. Erdinç, and N. G. Paterakis, “Power system protection with digital overcurrent relays: A review of non-standard characteristics,” in *Elect. Power Syst. Res.,* vol. 164, pp. 89–102, 2018.

[16] M. Bahrami, M. Fotuhi-Firuzabad and H. Farzin, "Reliability Evaluation of Power Grids Considering Integrity Attacks Against Substation Protective IEDs," in *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1035-1044, Feb. 2020.

[17] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, “Intruders in the grid,” IEEE Power Energy Mag., vol. 10, no. 1, pp. 58–66, Jan./Feb. 2012.

[18] C. -W. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos and A. Ginter, "Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems," in *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4405-4425, Sept. 2018.

[19] ABB, "Protection and Control IED Manager PCM600," ABB. [Online]. Available: https://new.abb.com/medium-voltage/digital-substations/software-products/protection-and-control-ied-manager-pcm600.

[20] ABB, "OpenSSL Heartbleed Vulnerability in Relion 650 series Ver. 1.3.0," ABB-VU-PSAC-1MRG016162, 2014. [Online]. Available: https://search-ext.abb.com/library/Download.aspx?DocumentID=1MRG016193&LanguageCode=en&DocumentPartId=&Action=Launch.

[21] Cybersecurity & Infrastructure Security Agency (CISA), "ICS Advisory (ICSA-22-333-02): Vulnerability in [specific vulnerability or device]," *CISA*. [Online]. Available: https://www.cisa.gov/news-events/ics-advisories/icsa-22-333-02.

[22] J. L. Sarralde and J. M. Yarza, “Cyber security applied to P&C IEDs,” in Proc. IEEE Power Energy Soc. Conf. Expo., 2014, pp. 1–5.

[23] M. Fischer, S. Tenbohlen, M. Schafer and R. Haug, "Determining power transformers' sequence of service in power grids," in *IEEE Trans. Dielectr. Electr. Insul.*, vol. 18, no. 5, pp. 1789-1798, October 2011.

[24] R. Billinton and R. N. Allan, Reliability Evaluation of Engineering Systems. Boston, MA, USA: Springer, 1992.

[25] E. Karangelos and L. Wehenkel, "Cyber–physical risk modeling with imperfect cyber-attackers," *Electr. Power Syst. Res.,* vol. 211, p. 108437, 2022.

[26] P. M. Subcommittee, “IEEE reliability test system,” IEEE Trans. Power App. Syst., vol. PAS-98, no. 6, pp. 2047–2054, Nov. 1979.

[27] Y. Zhang, A. Sprintson, and C. Singh, “An integrative approach to reliability analysis of an IEC 61850 digital substation,” presented at the IEEE Power Energy Soc. General Meeting, San Diego, CA, USA, 2012.