Factor of Security (FoS): Quantifying the Security Effectiveness of Redundant Smart Grid Subsystems

Onur Duman, Mengyuan Zhang, Lingyu Wang, Mourad Debbabi, Ribal Atallah, Bernard Lebel
Computer Security Laboratory, Concordia Institute for Information Systems Engineering
Concordia University, Montreal, Quebec, Canada,
Email: {o_dum, mengy_zh, wang, debbabi}@ciise.concordia.ca

***Abstract*—According to IEC (International Electrotechnical Commission) 61850-90-4, most smart grid substations are designed with redundancy in order to improve their availability in case of failures. Redundancy usually takes the form of having multiple subsystems with identical functionality based on the assumption that failures in one subsystem are isolated from other subsystems. However, this is not necessarily true in the case of failures caused by malicious attacks, because attackers can easily reuse their skills and tools across different subsystems under similar configurations. Taking this into consideration, this paper introduces the factor of security (FoS) metrics to quantify the security effectiveness of redundant subsystems in smart grids. Specifically, we first apply the attack graph model to capture various threats in smart grids and substations; we then formally define the FoS metric and the probabilistic FoS metric; finally, we evaluate those metrics under different scenarios through simulations.**

I. Introduction

By integrating information and communication technologies, smart grids could potentially enhance the efficiency and reliability of future power systems [1]. Such a capability grants smart grids an important role in addressing the global challenge that the demand for energy is growing faster than its supply [2]. On the other hand, the smart grid is a complex system involving many components for the generation, transmission, and distribution of energy to the end users. In particular, substations, which are responsible for protecting, monitoring and controlling the power system, represent one of the most critical components in a smart grid. This has been demonstrated in a study by the FERC (Federal Energy Regulatory Commission) which shows a coordinated attack on just nine substations (out of 55,000) can bring down the entire US (United States) power grid [3]. Also, in the real world attack on the Ukrainian power grid, which resulted in a blackout affecting 225,000 customers and lasted for several hours [4], substations were also among the main targets.

To make things worse, the relatively higher level of automation inherent to smart grids and substations [5] could render them an especially attractive target of the so-called *zero-day attacks*, which exploit previously unknown or unpatched vulnerabilities. *Zero-day attacks* are usually behind today's high profile security incidents against critical infrastructures (e.g., the aforementioned Ukrainian attack [4] and the Stuxnet attack [6]). Therefore, protecting smart grids and substations means more than just patching known vulnerabilities and deploying traditional defense mechanisms (e.g., firewalls, IDSs (intrusion detection systems), and intrusion prevention systems). Going beyond those to further evaluate the resilience of smart grids and substations against potential *zero-day attacks* is equally important.

A widely adopted solution to improve the resilience of smart grids in case of failures is to design them with redundancy. As indicated in IEC 61850-90-4 [5], the design of most smart grid substations includes redundant subsystems with identical functionality, such that failures of one subsystem can be easily tolerated by activating another subsystem. However, while such a solution might work well in the case of natural failures, which tend to be isolated among subsystems, the effectiveness of this approach towards malicious attackers has been neglected. This is because attackers can reuse reconnaissances gathered during the attack to compromise other similarly configured subsystems. Consequently, not all designs of redundant subsystems are equally effective against security attacks. Therefore, it would be futile to improve a design before a quantitative method of the effectiveness of security among substations is properly defined, since "you can not improve what you can not measure" [7]. Therefore, an important question arises, i.e., *How can we quantify the security effectiveness of a system design with redundant subsystems?*

To this end, most existing works are insufficient as they either ignore the redundancy aspect or are qualitative in nature (a detailed review of related work will be given in Section VI). Among the standardization for substations, IEC 61850 provides high-level guidelines to establish communication among devices from various manufacturers without elaborating on the security design. IEC 62351 is designed to provide security protection on top of IEC 61850 although it lacks a quantitative approach and is also criticized for other weaknesses [8]. For instance, Strobel *et al.* show two weaknesses in IEC 62351, one that allows GOOSE (Generic Object Oriented Substation Events) and SV (Sampled Values) messages to be replayed, and another in the time synchronization protocol which can lead the substation into a vulnerable state [8]. Although IEC 62443 [9] provides a set of requirements for security risk assessment, there still lacks a quantitative and credible validation [10]. Security metrics in the context of smart grids have been investigated previously. As an example, in [11], the authors analyze four different attacks against SCADA (Supervisory Control and Data Acquisition) systems and apply the mean time to compromise metric to those attack scenarios [11]. In [12], the authors develop attack graph-based security metrics to identify critical components. In [13][14], the authors perform a cyber-physical contingency analysis by taking malicious compromises into account in addition to natural failures. There is also rich literature on redundancy and security in control systems. For instance, in [15] the authors study the problem of structural controllability and propose repair strategies for control systems and in [16], the authors define control areas which are vulnerable to attacks. On the other hand, improving security using redundancy mechanisms has also received significant attentions, e.g., the n-variant system [17] and the behavioral distance-based detection [18], although most existing works do not employ an explicit security metric like in our work. To the best of our knowledge, we are among the first to focus on quantifying the security effectiveness of redundant subsystems against both known and zero-day vulnerabilities in smart grids.

In this paper, we introduce a novel security metric, namely, FoS (Factor of Security) , to quantify the security effectiveness of redundant subsystems in smart grids[1]. Our key idea is the following. Although not seen in the context of smart grids or cyber-physical security, the factor of safety is a widely used concept in traditional engineering domains such as mechanical design which, roughly speaking, measures how much stronger a system is than it needs to be. For example, the factor of safety would be two if the designed load carrying capacity (called the *strength*) is twice as much as the actual load (called the *stress*). We adopt this concept to the context of cyber-physical security in redundant smart grid subsystems. Specifically, we first design a representative smart grid substation configuration based on IEC 61850-90-4 and existing industrial practices, which provides concrete details about the hardware and software components to facilitate the threat modeling process. Second, on the basis of the well-known attack graph model, we define the strength and stress of a smart grid system as the length of the shortest attack path for the smart grid, and its subsystems, respectively; the ratio between the two then yields the *FoS*, which intuitively gives the equivalent number of subsystems in terms of resilience to attacks.

The preliminary version of this paper has appeared in [19], which has been significantly extended in this paper. The major extensions include the following. First, we further define the PFoS (Probabilistic Factor of Security) metric based on the Bayesian network-based attack graph model, in order to capture not only the worst case (captured by FoS) but also the average case in which attackers would not necessarily follow the shortest paths (Section III). Second, we have extended our previous models to cover both known and zero-day vulnerabilities in a unified manner, and also to cover both the smart grid and substation level applications. We have modified our models to include security components such as firewalls and IDSs, as well as redundancy measures (Section IV). Third, we have performed additional simulations to evaluate both metrics, and also introduced a new series of simulations using the IEEE 14 bus system in order to evaluate the metrics at the smart grid level (Section V).

In summary, our main contributions are as follows:

- To the best of our knowledge, this is the first effort on formally quantifying the security effectiveness of redundant subsystems in the context of smart grids. We are also among the first to adopt the factor of safety concept from traditional engineering domains to security.
- As evidenced in the simulation results, the proposed metrics can be applied by security practitioners to answer practical questions for better understanding and mitigating the security threats of both known vulnerabilities and zero-day attacks.

The remainder of this paper is organized as follows. Section II describes a detailed substation design based on IEC 61850-90-4. Section III details the design of our metrics. Section IV applies metrics to various attack scenarios. Section V gives simulation results. Section VI reviews the literature and Section VII concludes the paper.

II. Designing Smart Grid Substation based on IEC 61850

A key challenge facing the development of security metrics and threat models for smart grids is the lack of public accesses to the concrete design of real world smart grids including detailed information about the hardware and software components and their vulnerabilities. This is understandable since smart grid operators would be reluctant to disclose details about their infrastructures and especially the vulnerabilities. Although existing standards like IEC 61850-90-4 provide sample substation configurations [5], those configurations are typically very simplistic and only contain high-level concepts, which is insufficient for our purposes. Therefore, we first present a concrete design of a smart grid substation with redundant subsystems to facilitate further discussions. To ensure the design is sufficiently representative, it is based on IEC 61850-90-4 and product documentations from key vendors including ABB [20], SEL [21], and Symmetricom [22].

Specifically, Figure 1 shows a substation with two redundant subsystems, A and B. The numbers inside circles ranging from $A1$ to $A27$ are components of subsystem A and numbers from $B1$ to $B27$ are components of subsystem B. In subsystem A, the component $A2$ is protected by a firewall, namely F_A, since it is a critical component. Similarly, in subsystem B, the component $B2$ is protected by the firewall F_B. Components $A7 - A13$ are monitored for anomalies by an IDS, namely, IDS_A_1 [23]. Similarly, components $A17 - A23$ are monitored by IDS_A_2. Same applies to components belonging to subsystem B, and they are monitored by IDS_B_1 and IDS_B_2. For components for which a replica exists, the component and its replica are numbered correspondingly, e.g., $A1$ is the replica of $B1$ (for those which are not replicated, both numbers refer to the same component, e.g., $A4$ and $B4$). We assume substations communicate with the control center (*node* 300) through WAN (Wide Area Network), which

[1] Although we focus on smart grids, the FoS metrics may potentially be applied to other cyber or cyber-physical systems designed with redundancy.

is also used by remote operators (*node* 200) to manage the substation remotely. Also, the attacker (*node* 100) is assumed to be connected to the WAN, which can be either an insider or an outsider with unauthorized accesses to the WAN.

According to IEC 61850-90-4 [5], a substation is divided into three levels as detailed in the following:

- **Substation Level:** HMI (Human Machine Interface) is used for monitoring the status of the substation (*nodes* $A1$, $B1$). Workstations (*nodes* $A2$, $B2$) are used for automation in a substation. According to IEC 61850-90-4, workstations at the station level can be used as SCADA servers. Since SCADA servers are critical components [11], incoming and outgoing connections to those are protected by firewalls F_A and F_B. GPS (Global Positioning System) clocks (*nodes* $A3$, $B3$) are used for time synchronization in the substation. All connections to the substation go through substation gateways (*nodes* $A6$, $B6$).
- **Bay Level:** According to IEC 61850-90-4, the bay level mostly contains IEDs (Intelligent Electronic Devices). IEDs are used to improve the automation inside a substation [24]. IEDs in bay A_1 and bay B_1 control field devices which are connected to Process Bus 1, and IEDs in bays A_2 and B_2 control field devices which are connected to Process Bus 2. The IEDs in those bays act as interfaces between cyber components (components at the substation level) and physical components (components at the process level). Each bay contains protection IEDs (*nodes* $A7$, $B7$, $A17$, $B17$), which are used for fault isolation. Control IEDs (*nodes* $A8$, $B8$, $A18$, $B18$) are used for managing the power system for efficient usage. In IEC 61850-90-4 [5], there are also IEDs for power quality measurement, which are included in our design as power quality measurement IEDs (*nodes* $A9$, $B9$, $A19$, $B19$). Even though not seen in IEC 61850-90-4, PMUs (Phasor Measurement Units) connected to PDCs (Phasor Data Concentrators) are also included in our design since it can be seen in the sample substation design provided by SEL [21]. The PMUs (*nodes* $A10$, $B10$, $A11$, $B11$, $A20$, $B20$, $A21$, $B21$) and PDCs (*nodes* $A12$, $B12$, $A22$, $B22$) inside the bays are used for obtaining synchronized measurements of voltages and phase angles. Lastly, each bay is monitored using an IDS (IDS_A_1, IDS_A_2, IDS_B_1, IDS_B_2).
- **Process Level:** The process level contains field devices, e.g., voltage transformers (*nodes* $A14$, $B14$, $A24$, $B24$), current transformers (*nodes* $A15$, $B15$, $A25$, $B25$), and circuit breakers (*nodes* $A16$, $B16$, $A26$, $B26$). All the devices receive commands from IEDs and send measurements to IEDs. Some of those devices (*nodes* $A24 - A26$, $B24 - B26$) must be connected to a merging unit (*nodes* $A27$, $B27$) before being connected to the process bus.

Table I summarizes the role of each component with relevant references including standards and research papers which address such components. To make the design more representative, Figure 1 also reflects many concepts of industrial practices, e.g., SEL [21], Symmetricom [22], ABB [20], etc., as detailed below.

- The design includes two PMUs (*such as nodes* $A10$, $A11$) connected to one PDC (*such as node* $A12$) in each bay, which is based on a similar configuration by SEL [21].
- The design includes three different field devices, including voltage transformer, current transformer, circuit breaker, and their intelligent counterparts. Intelligent devices (*nodes* $A14$, $B14$, $A15$, $B15$, $A16$, $B16$) can be directly connected to the process bus. Other devices (*nodes* $A24$, $B24$, $A25$, $B25$, $A26$, $B26$) need to first go through a merging unit (*nodes* $A27$, $B27$) before being connected to the process bus. This design is based on a similar configuration given by Symmetricom [22].
- The design includes two subsystems with equivalent functionality, with everything replicated except the event printer (*nodes* $A4$, $B4$) and the event logger (*nodes* $A5$, $B5$). This is based on a similar configuration given by ABB [20] in which the HMI (*nodes* $A1$, $B1$) and the GPS server (*nodes* $A3$, $B3$) are replicated.
- The design includes two firewalls (one for each subsystem) in the substation level and includes IDS in each bay. This is based on a similar configuration given by [23].

In addition to hardware components of the detailed configuration, we also assume the following services are running on top of those components. The GATEWAY service runs on substation gateways (*nodes* $A6$, $B6$). The HMIs and workstations run the SSH (The Secure Shell) service for remote maintenance. They also run HTTP (HyperText Transfer Protocol) service to provide a user-friendly interface to substation operators. Workstations can also be used as SCADA servers. GPS clocks run GPS service for time synchronization inside the substation. Services running on IEDs have the same names as the names of the IEDs (such as protection service on protection IEDs). The remote operator's machine is running HTTP and SSH.

III. Defining the Factor of Security Metrics

In this section, we first discuss a motivating example to build intuitions, and then we formally define the FoS (Factor of Security) and PFoS (Probabilistic Factor of Security) metrics.

A. Motivating Example

For the substation depicted in Figure 1, it may seem obvious that, since the substation has two separate subsystems, any faults causing one subsystem to fail can be easily tolerated by switching to the other unaffected subsystem without causing a power outage. However, such a reasoning only works for faults that happen naturally in a random fashion. The situation would be quite different when it comes to malicious attacks. For example, consider a remote attacker who wishes to cause a blackout to an area, and he/she has identified this substation as his/her main target. This attacker is an outsider who performs his/her attacks through vulnerability exploitations. Subsystem A is the actively running system, and the attacker targets

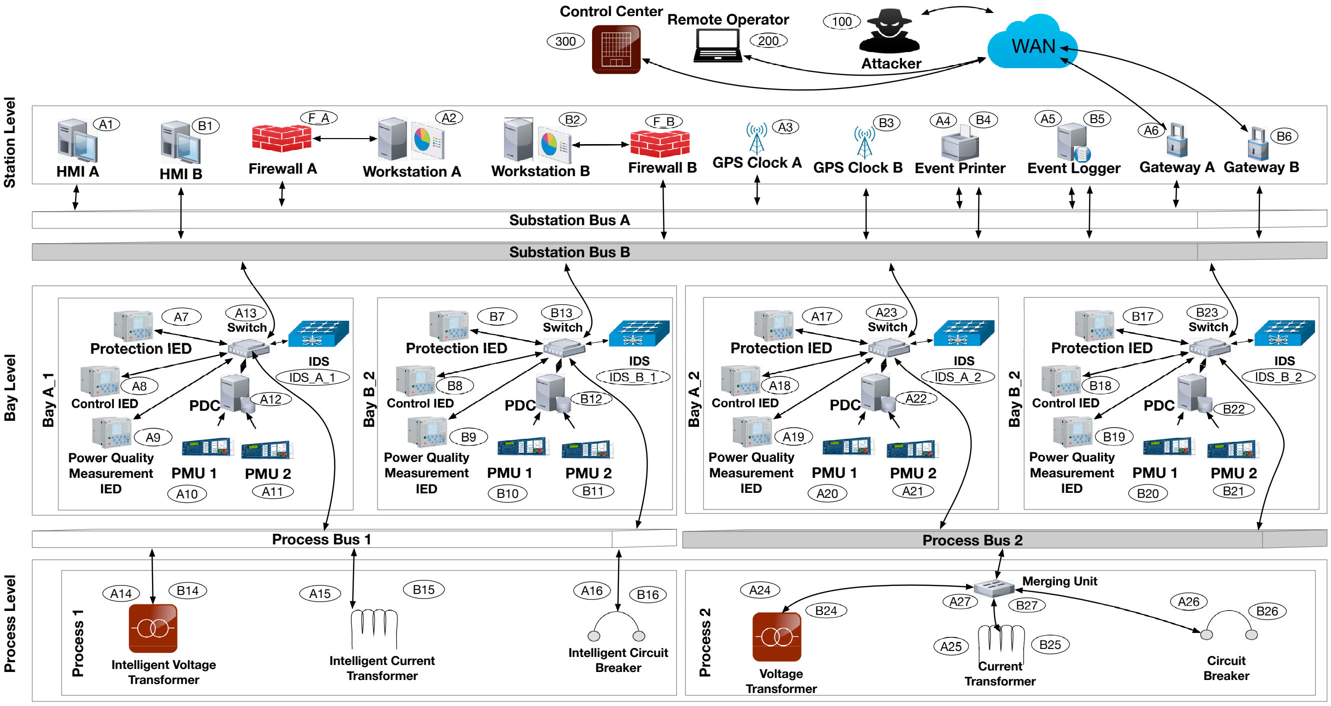


Fig. 1: Smart Grid Substation Based on IEC 61850-90-4

the HMI in subsystem A (node $A1$) by getting administrator access (such as root in Linux machines) in the node $A1$. In order to achieve this, the attacker needs to first compromise the substation gateway (node $A6$) by exploiting a known or zero-day vulnerability in the substation gateway. After that, the attacker needs to compromise the HMI (node $A1$) through another vulnerability exploitation. As a consequence, the attacker needs to exploit two vulnerabilities in order to gain administrator access in HMI. Suppose the operator notices that subsystem A is under attack and switches to subsystem B before the attacker could start to remotely trip circuit breakers [11]. Now the attacker might notice that, although the actively running subsystem has been changed, subsystem B still contains the identically configured components, namely, the gateway (node $B6$) and HMI (node $B1$). Exploiting the same vulnerabilities, the attacker will succeed in compromising subsystem B and subsequently bring the substation down and cause a major power outage. Clearly, even though the substation has been designed to include two subsystems, similar vulnerabilities shared by those subsystems mean that these do not really count as two subsystems in terms of their resilience to malicious attacks, since compromising the substation requires almost the same effort and skill as compromising one subsystem.

To better capture such intuitions, we apply the concept of *Factor of Safety*. Although not seen in the context of the cyber-physical security of smart grids, the factor of safety is a widely used concept in traditional engineering domains, such as mechanical design [47]. Roughly speaking, the factor of safety of a system measures how much stronger the system is designed to be (e.g., an airplane is designed with two engines), than it needs to be (e.g., one engine is actually sufficient), in order to ensure the desired level of reliability (e.g., the failure of one engine can be safely tolerated). More formally, the factor of safety is defined as the ratio between the designed load carrying capacity (i.e., the maximum amount of load that can be carried by the system, namely, the *strength*), and the actual load (i.e., the expected amount of load to be carried by the system, namely, the *stress*), denoted as $Factor\ of\ Safety = \frac{Strength}{Stress}$ [47]. Intuitively, by applying this concept to our previous example, we know that our substation would have a factor of safety less than 2 from the security point of view (i.e., the substation is not twice as secure as it needs to be).

B. Threat Model

The following describes different aspects of our threat model.

- **Type of Attackers:** We focus on remote attackers who rely on network connections to launch their attacks and escalate privileges through exploiting either known or zero day vulnerabilities in the smart grid components. Therefore, attacks that do not rely on vulnerabilities but employ social engineering, insider misbehavior, or manipulating smart grid measurements [30] will not be considered.
- **Attacker's Capacity and Access Level:** In the substation level, we consider attacks performed through exploiting vulnerabilities. The attacker can exploit known or zero-day vulnerabilities in order to escalate their privileges. The attacker initially does not have any access to any devices in the substation except the substation gateway. Whereas, in the smart grid level, we focus on attacks performed by disconnecting transmission lines through

Level	Component	Functionality	References
Substation Level	Gateway (A6, B6)	Sends data to the control center, transfers commands received from the control center [25], and allows remote operators to connect to the substation for monitoring and controlling [26].	IEC 61850-7-1 Clause 8.2.3, [1],[11], [19], [23]
	HMI (A1, B1)	Presents information to the operator about the state of the substation [27].	IEC 61850-7-1 Clause 7, [4], [11], [19], [23], [28], [29]
	Workstation (A2, B2)	Performs automation in a substation, and is also used as a SCADA server [11].	IEC 61850-7-1 Clause 5.2, IEC 62264-1:2013, [1], [4], [6], [8],[10], [11], [12], [19], [23], [24], [30], [31], [32], [29], [33]
	GPS Clock (A3, B3)	Time source in the substation for time synchronization between devices [28].	IEEE 1588-2019, [19], [23], [24], [28], [34], [35]
	Event Printer(A4, B4)	Devices in a substation produce time stamped events (such as tripping), which are sent to the event printer for monitoring [36].	IEC 61850-90-4 Clause 7.1, [19], [29]
	Event Logger (A5, B5)	Event logger for logging status changes in substation IEDs [37].	IEC 61850-90-4 Clause 7.1, [4], [19], [24]
Bay Level	Protection IED (A7, B7, A17, B17)	Detects electrical faults and performs fault isolation [38].	IEC 61850-7-1 Clause 5.4, [1], [11], [13], [14], [19], [24], [28]
	Control IED (A8, B8, A18, B18)	Manages the power system for efficient usage and regulates system parameters [38].	IEC 61850-90-4 Clause 7.3, [1], [11], [19], [23], [24], [28], [33]
	Power Quality Measurement IED (A9, B9, A19, B19)	Monitors the power quality [5].	IEC 61000-4-30, [11], [19], [23]
	PMU (A10, A11, B10, B11, A20, A21, B20, B21)	Obtains synchronized measurements of voltage magnitudes and phase angles [39].	IEC 61850-90-5 Clause 6.3, C37.118.2-2011, [1], [19], [24], [30], [35], [31]
	PDC (A12, B12, A22, B22)	Receives, combines and pre-processes synchronized measurements [40].	IEC 61850-90-5 Clause 6.4, C37.118.2-2011, [1], [19]
Process Level	Voltage Transformer (A14, B14, A24, B24)	Measures voltage [41].	IEC 60044-7, [1], [11], [19], [31], [42]
	Current Transformer (A15, B15, A25, B25)	Steps down current levels and measures them [43].	IEC 61869 Part 1, [1], [2], [11], [19], [31], [42]
	Circuit Breaker (A16, B16, A26, B26)	Connects or disconnects transmission lines [44].	IEC 61850-8-1 Clause 6.4, IEC 61850-7-1, Clauses 11.2,12.1, [1], [4], [11], [12], [13], [14], [19], [45], [31], [42]
	Merging Unit (A27, B27)	Converts analog signals into IEC 61850 Sampled Value (SV) [46].	IEC 61850-7-1 Annex B, [19], [23], [31]

TABLE I: Details of Components in Our IEC 61850 Substation Design

tripping circuit breakers or disrupting communication lines.

- **Zero-Day Vulnerabilities:** Zero-day vulnerabilities [48] are unknown vulnerabilities whose existence and the way to exploit are unknown. Attackers are assumed to be able to exploit those.
- **Known Vulnerabilities:** Known vulnerabilities can be exploited as long as all preconditions are satisfied. As an example, a known vulnerability in Apache HTTP server, with identifier CVE (Common Vulnerabilities and Exposures)-2010-1151 [49], allows the attacker to create a race condition and bypass the authentication. If an Apache HTTP server has that vulnerability and if the attacker can connect to that web server and if the attacker has at least user privilege on the web server, then the attacker can exploit that vulnerability to bypass authentication and escalate her privilege. In our analysis, tools and technologies used by the attacker are not relevant since they are not part of attack graphs.
- **Assumptions:** As an assumption of the attack graph model, the attackers are assumed to have all the required capabilities and attacking tools to exploit vulnerabilities as long as all preconditions are satisfied. We assume a series of redundant subsystems will be launched in a linear manner (in any order) after each failure and the attacker must compromise all the subsystems before causing substantial damages (e.g., a blackout). The attacker is assumed to reuse any knowledge or skills he/she may have gained during exploiting a vulnerability to attack other similar components in one or more subsystems. We focus on attacks that aim at taking control of critical assets (e.g., circuit breakers) in smart grids, and thus we ignore any reconnaissance steps but consider that attackers already have sufficient knowledge about the smart grid.

C. Redundant Attack Graph Model

To realize this idea, we first need to model the (both known and unknown) vulnerabilities inside a smart grid or substation, the causal relationships between such vulnerabilities (e.g., exploiting the HMI is only possible after exploiting the gateway in Figure 1), and possible ways for compromising the critical assets (e.g., the circuit breakers). To this end, we employ the widely used attack graph model [50], [51]), which is a directed graph with two types of nodes (i.e., exploits and conditions) and edges pointing from pre-conditions to exploits and from exploits to post-conditions. The conditions that are not post-conditions of any exploit are called the initial conditions and assumed to be satisfied initially (i.e., before any exploit occurs), whereas the sink nodes of the attack graph (which represent the critical assets) are usually called the goal conditions. An exploit can be satisfied if and only if all of its pre-conditions are satisfied and satisfying an exploit leads to the attacker gaining its post-conditions. Redundant attack graph contains two or more attack graphs merged using an intermediate node. Definition 3.1 gives the formal definition of the redundant attack graph.

Definition 3.1: (Redundant Attack Graph) Given a network with set of hosts H, set of services S, with the service mapping *ser(.):* $H \rightarrow 2^R$, set of exploits $E = \{ \langle r,\ h_s,\ h_d \rangle \mid h_s\ \epsilon\ H,\ h_d\ \epsilon\ H, r\ \epsilon\ ser(h_d)\}$, and their pre- and post-conditions C, a redundant attack graph is a directed acyclic graph $G\ (\ E\ \bigcup C, R_r\ \bigcup\ R_i\ )$ where $R_r\ \subseteq\ C\ \times\ E$ and $R_i\ \subseteq\ E\ \times\ C$ are pre- and post-condition relations respectively.

Our redundant attack graphs can be generated in a similarly way as regular attack graphs [50], [51]. Attack graph generation is conducted in three stages [52] which are reachability analysis, attack graph modeling and core attack graph building. Reachability analysis determines direct reachability between network hosts. Attack graph modeling involves creating attack templates which involve conditions (capabilities required by the attacker to succeed) for attacking network assets and relationships between conditions and network elements. Attack graph building phase refers to algorithms used to build attack graphs. As an example, MulVal [53] is an open source tool for attack graph generation and it models exploits as logic propositions and applies logic deduction to reach goal facts from initial facts.

Figure 2 gives an example of our *redundant attack graph model*. In Figure 2, each triple inside an oval indicates an exploit $\langle vulnerability, source\ host, destination\ host \rangle$ (such as $\langle v\_SSH, 100, 200 \rangle$) and each pair in clear text indicates a condition (e.g., a connectivity relationship such as $\langle 100, 300 \rangle$, and a service running on a host such as $\langle SSH, 300 \rangle$). The nodes at the top are examples of initial conditions (such as $\langle Attacker, 100 \rangle$), whereas the node at the bottom is the goal condition (which is $\langle TimeDelay, \{A3, B3\} \rangle$). In addition to the standard notations used in attack graphs [54], [55], we introduce some new notations. First, the double oval nodes represent network services with no known vulnerabilities. Such network services are considered to contain potential zero-day vulnerabilities. Second, we attach a version number to those nodes, shown in square brackets, to distinguish between different variations of the same service (e.g., Apache [56] or IIS (Internet Information Services) [57] for the HTTP service). Third, oval nodes with CVE [58] numbers (such as $\langle V\_TRIP, ATTACKER, T2\_1 \rangle$ in Figure 5) represent known vulnerabilities. Fourth, firewalls ($\langle v\_Firewall, A6, FA \rangle$) are shown in red and represented in the same way as exploits since from the attackers' perspective bypassing the firewall also requires exploiting a vulnerability in the firewall. The postcondition of the firewall is the connectivity behind that firewall (such as connectivity condition $\langle A6, A2 \rangle$ is behind the firewall F_A). The firewall has only one precondition which is the name of the firewall (such as $\langle Firewall, F\_A \rangle$). Lastly, the attack graph model in Figure 3 contains intrusion detection nodes ($\langle v\_IDS, A7, IDS\_A\_1 \rangle$ and $\langle v\_IDS, B7, IDS\_B\_1 \rangle$). The postcondition of those nodes is the failure condition (which is $\langle Fail, Attacker \rangle$). The preconditions of an intrusion detection node include the detection condition (such $\langle IDS\_A\_1, Detect \rangle$) which means that the IDS has succeeded in detecting the attack. The stage in which the attack is detected can be any postcondition of any vulnerability exploit (the privileges acquired by the attacker). If the attack has been detected in the final stage, another condition with the name "Attacked" is added. The preconditions of an IDS also include the existence of the IDS (such as $\langle IDS\_A\_1, A7 \rangle$), meaning that the node $A7$ is being monitored by an IDS with name IDS_A_1. If the fact that the attacker has acquired a privilege is not detected by IDS, then the movement by the attacker to acquire the detection condition is stealthy.

Another challenge in applying the attack graph model in our context is to model the existence of multiple subsystems and their relationships. In Figure 2, both sub-graphs for the subsystems share the same topology since subsystems are usually designed as replicas of each other. One subsystem is active each time and all others are used as backups. Since the operator will switch an active subsystem under attack to another backup subsystem, ideally the attacker would have to compromise all subsystems before he/she can bring down the entire smart grid or substation. In this sense, the relationship between those subsystems is a conjunction, which can be modeled using an intermediate exploit (e.g., node I in Figure 2), which takes the goal condition of each subsystem as its pre-condition and the final goal condition as its post-condition. The probabilities, the common parent nodes and the similarity node in Figure 6 can be ignored for now and will be discussed later.

D. Factor of Security

Following our discussions of the motivating example, we now consider how to more precisely capture those intuitions. Our key idea is to define the aforementioned ”load” concept (which is used to define both the strength and stress of a system and hence its factor of safety) as the system's level of attack resilience. To that end, we apply an existing network security metric, the K-zero day safety metric ($k0d$) [55] to quantify the level of attack resilience. Considering each remotely accessible service to potentially contain an unknown vulnerability, the $k0d$ metric basically counts the minimum number of such vulnerabilities required to compromise a given network asset. A larger $k0d$ value indicates a more secure network because it is less likely for a large number of unknown vulnerabilities to co-exist and be exploitable by the same attacker. Armed with this concept, we can define the ”strength” as the $k0d$ value of the entire smart grid or substation system with the existence of all redundant subsystems taken into consideration, and the ”stress” as the $k0d$ value of a subsystem (without considering redundancy). The ratio of the two thus indicates how much more security is provided by the design of redundant subsystems than what is provided by each subsystem. We provide more details in the following.

1) The Factor of Security Metrics: To define the factor of security metrics based on the redundant attack graph model, we consider three cases.

a) Case 1: We start with the simplest case, i.e., there is no known vulnerability (only zero-day vulnerabilities) and we are only worried about the attackers who can compromise the critical assets with the minimum effort. We first define the *strength* of a smart grid or substation with respect to a given critical asset as the $k0d$ value for the whole system calculated based on the redundant attack graph model with the final goal condition. This definition indicates the level of security resilience in terms of the least number of distinct zero-day vulnerabilities required for compromising the whole system, i.e., all the subsystems. Second, we define the *stress* of the system as the maximum $k0d$ value of a subsystem with respect to the same critical asset. We choose the maximum value in order to ensure a proper range of values for the factor of security, which will never exceed the number of subsystems as designed. Finally, we define the *FoS (Factor of Security)* as the ratio between the strength and the stress, which intuitively indicates how many subsystems a substation effectively has from the security perspective. In an ideal case, the factor of security should be equal to the number of subsystems physically present in the substation. A lower factor of security value indicates a less-than-ideal design in which the redundancy does not deliver as much security resilience as it is designed to. More formally, the strength of a system S with multiple subsystems S_i for a given asset μ (μ_i in S_i) is defined as $Strength(S,\mu) = k0d(S,\mu), \mu = \bigcup_{i=1}^{N} \mu_i$. The stress is defined as $Stress(S,\mu) = \max_{\forall S_i} k0d(S_i,\mu_i)$. Taking stress and strength, the factor of security is defined as:

$$Factor\ of\ Security\ (S,\mu) = \frac{Strength(S,\mu)}{Stress(S,\mu)} \quad (1)$$

The factor of security, which is defined as $FoS(S,\mu) = \frac{k0d(S,\mu)}{max\ (k0d(S_i,\mu_i))}$, where $i = 1 \cdots n$, and n is the number of subsystems, is a semi-metric function since it satisfies the following properties of a semi-metric function [59]:

- **Self identity:** $FoS(S,\mu) = 0$ iff $k0d(S,u) = 0$, and since $k0d$ satisfies self identity as proven in [55], FoS also satisfies self identity.
- **Positivity:** $FoS(S,\mu)$ satisfies positivity since both $k0d(S,\mu)$ and $max(k0d(S_i,\mu_i))$ are positive and $k0d$ satisfies positivity [55].
- **Symmetry:** $FoS(S,\mu)$ satisfies symmetry since both $k0d(S,\mu)$ and $max(k0d(S_i,\mu_i))$ satisfy symmetry [55].

b) Case 2: In the second case, we consider the co-existence of known vulnerabilities [60] and zero-day vulnerabilities [55]. Compared to zero-day vulnerabilities, which are typically less common and known to fewer attackers, known vulnerabilities are much easier to exploit; equivalently, they provide much less attack resilience from the defender's perspective, and should count less than a zero-day vulnerability (which counts as 1 in calculating the $k0d$ metric). The probability of successfully exploiting a known vulnerability should reflect the relative difficulty of exploiting that vulnerability [60]. Instead of assigning arbitrary values, we employ the standard CVSS (Common Vulnerability Scoring System) scores of known vulnerabilities [61], which are readily available in the public vulnerability database (which is updated frequently and can be accessed through [62] or accessed through an API (Application Programming Interface) from [58]). CVSS measures the impact of each individual vulnerability and it also contains environmental metrics [63]. We normalize the CVSS score of a known vulnerability (which ranges between 0.0 and 10.0) in order to convert the vulnerability score to a probability of exploiting the vulnerability as: $\frac{CVSS}{10.0}$, which is usually called the attack likelihood (or probability) of the vulnerability. As an example, the probability of a known vulnerability CVE-20120-0022 (used later in our discussions) is 0.5 (the CVSS score is 5.0). For zero-day vulnerabilities, we follow the existing approach [60] of modeling them as a special kind of vulnerabilities with following CVSS base metrics: remediation level "unavailable", report confidence "unknown", and exploitability "unproven that exploit exists". With those values as inputs to the CVSS equation [61], the CVSS score is calculated as 0.8 and therefore a nominal probability 0.08 is assigned to zero-day vulnerabilities. Finally, with probabilities obtained for both known and zero-day vulnerabilities, we can then convert each exploit of a known vulnerability into an equivalent number of exploits of zero-day vulnerabilities, and use the result inside the same calculation of the FoS metric as in the above Case 1 using Equation 1.

$$log_{0.08}(Probability\ of\ the\ Vulnerability) \quad (2)$$

c) Case 3: The previous two cases are based on the worst case scenario (from the defender's point of view) which provides a useful lower bound for the level of security resilience against the best attackers who can always follow the shortest paths. In the last case, we consider other attackers who may not (be able to) follow the shortest path, and we propose an average case-based metric, called the *PFoS (Probabilistic Factor of Security)*. For this purpose, we adopt the Bayesian network-based attack graph model introduced in [54]. We first construct a Bayesian network using the attack graph as the DAG (Directed Acyclic Graph). The probabilities assigned to vulnerabilities (CVSS divided by 10 for known vulnerabilities and 0.08 for zero-day vulnerabilities) are interpreted as the conditional probabilities that the exploits of corresponding vulnerabilities can be executed given all the pre-conditions are already satisfied. Additional conditional probabilities also need to be defined to encode the logical AND and OR relationships between pre- and post-conditions. In addition, as shown in Figure 2, common parents are added to exploit nodes sharing the same vulnerabilities to represent the fact that, if one of those exploits is already executed, the rest would have a much higher conditional probability of being executed. To reflect this, for exploit nodes connected to a common parent, the conditional probability has a higher value (e.g., 0.9) when all of their preconditions (including the common parent node) are satisfied. Finally, in order to model two components which are similar but not identical (e.g., two versions of the software), we have introduced the similarity nodes (an example is shown in Figure 6).

Next, we perform Bayesian inferences based on the constructed Bayesian network as follows. We assign all initial conditions with probability 1 and calculate the probabilities of the goal condition inside each subsystem, and that of the goal condition of the entire system. We then use above Equation 2 to convert these probabilities into the equivalent number of zero-day exploits corresponding to the entire system, denote as $k0d_S$, and that of the i^{th} subsystem, denoted as $k0d_i$. Finally, the strength of a system S with multiple subsystems S_i for a given asset μ (μ_i in S_i) is defined as $Strength(S, \mu) = k0d_s$, and the stress is defined as $Stress(S, \mu) = \max_{\forall S_i} k0d_i$. With those definitions, the factor of security can be calculated as usual using Equation 1.

IV. Applying FoS to Smart Grids and Substations

In this section, we illustrate how our FoS metrics can be applied to both the smart grid substations and the smart grid distribution domain to evaluate the security effectiveness of redundant subsystems. Specifically, we apply the metrics to two substation specific attack scenarios, namely, the PTP (Precision Time Protocol) time delay attack [28] and the tripping circuit breakers attack [11], and two attack scenarios in smart grids, namely, the cascading link failure attack [45] and the coordinated attack against substations and transmission lines [64].

A. Attack Scenarios in IEC 61850 Substations

1) PTP Time Delay Attack: PTP is a protocol used to synchronize clocks in a network. The PTP time delay attack aims to delay PTP messages which are used for time synchronization in IEC 61850 substations [28]. Time synchronization among IEDs in substations is important since lack of time synchronization can lead to control center making wrong decisions such as scheduling the power demand inefficiently [34]. PTP requires a master clock, which acts as the main time source, and slave clocks, which get timing information from the master clock. In our substation model (Figure 1), the GPS clocks (nodes $A3$ and $B3$) are PTP masters for each subsystem. In order to attack this protocol, the attacker needs to delay or modify messages used in PTP for time synchronization [28]. The attacker could be located physically close to the substation such that he/she can utilize a GPS simulator to spoof GPS messages [35]. The attacker could also launch the attack through remotely accessing the substation, e.g., by compromising substation gateways (nodes $A6$ or $B6$) or by causing a malware to be installed on the remote operator's machine (node 200). In this scenario, we do not assume the physical proximity but consider the latter case.

Figure 2 shows our attack graph model for the PTP time delay attack. The attacker can either compromise the remote operator or the control center in order to gain access to the substation gateway. After compromising the substation gateway, the attacker needs to compromise the workstation and then the GPS server to cause a time delay. Therefore, to compromise each subsystem, the attacker needs to exploit totally five vulnerabilities (one in SSH version 1, SSH version 2, or HTTP version 1, followed by one in the gateway, one in workstation and one in the GPS server and also the firewall) to compromise each subsystem, and the $k0d$ value of each subsystem is 5 (since all vulnerabilities are assumed to be zero-day). On the other hand, in order to compromise the whole system, the attacker needs totally nine distinct vulnerabilities (one in SSH version 1, one in Gateway version 1, one in Gateway version 2, one in SCADA version 1, one in SCADA version 2, one in GPS version 1, one in GPS version 2, one in Firewall version 1, and one in Firewall version 2), so the FoS (Factor of Security) can be calculated as the following.

$$FoS = \frac{9}{max(\{5, 5\})} = 1.8$$

Observation: This simple application of the FoS metric can lead to the following observations. First, as it can be seen, the FoS value is less than two because part of the attack graph (exploits of the remote operator's machine or network services of the control center) is shared by both subsystems. The lesson is that, while it is common for redundant subsystems to share certain external components, such shared components may lead to common attack surface between the subsystems and hence reduce the overall security effectiveness. Second, we can see that diversity in the gateway (nodes $A6$ and $B6$) and GPS servers (nodes $A3$ and $B3$) between the two subsystems (i.e., the two subsystems are using two different versions of those services) is the key to improve the FoS value, even though diversifying such components may or may not be feasible in practice due to the implied costs.

For the calculation of the PFoS (Probabilistic Factor of Security), we perform Bayesian inference on the goal condition of each subsystem, which is $\langle TIME\_DELAY, A3\rangle$ and $\langle TIME\_DELAY, B3\rangle$, respectively, and on the goal condition of the whole system, which is $\langle TIME\_DELAY, \{A3, B3\}\rangle$. Probabilities for those nodes can be calculated as follows.

- Pr($\langle TIME\_DELAY, A3\rangle$) = 0.0000082037
- Pr($\langle TIME\_DELAY, B3\rangle$) = 0.0000082037
- Pr($\langle TIME\_DELAY, \{A3, B3\}\rangle$) = 0.0000000003

By taking those probabilities into account, PFoS can be calculated as follows.

$$\begin{aligned} L0 &\leftarrow log_{0.08}(0.0000082037) = 4.63665 \\ L1 &\leftarrow log_{0.08}(0.0000082037) = 4.63665 \\ L2 &\leftarrow log_{0.08}(0.0000000003) = 8.681549 \\ PFoS &= \frac{L0}{max(L1, L2)} = 1.87237 \end{aligned}$$

Observation: We can observe that, in contrast to the calculation of FoS, the strength and stress under PFoS both become

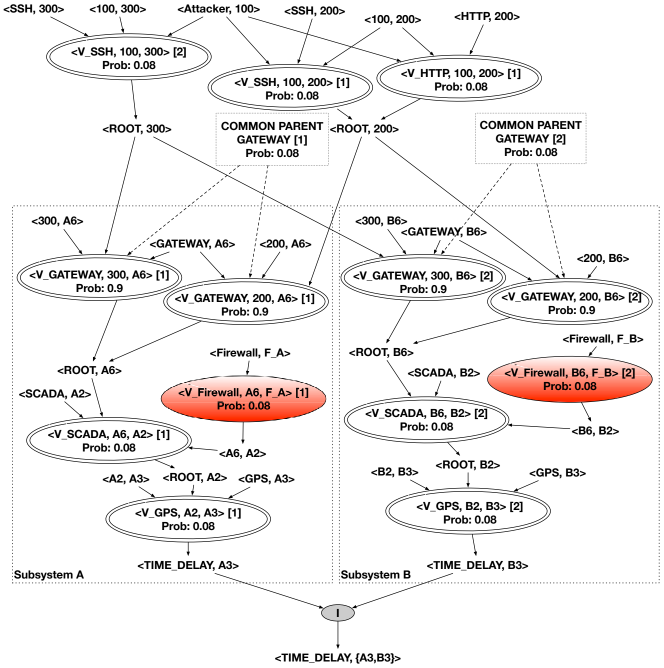


Fig. 2: Attack Graph For PTP Time Delay Attack

slightly less. This is mainly due to the existence of multiple attack paths, which is taken into consideration under PFoS, whereas only one (the shortest) path is considered under FoS. While the difference is not significant in this case (since there are only a few attack paths), in general, the two metrics may behave quite differently (hence it is important to consider both) especially when there exist a large number of attack paths. We will investigate this further through simulations in Section V.

2) Tripping Circuit Breakers Attack: Circuit breakers are responsible for protecting transmission lines from damages due to excess current. To illustrate, transmission line failures were seen in 2003 Northeastern blackout [65]; even though this blackout was not a result of a cyber attack, this could as well be the case since an attacker who has access to the substation HMI will be able to send trip commands remotely from the HMI to Protection IEDs [11]. In the Ukraine attack [4], attackers have tripped circuit breakers by sending remote commands, and they also have changed the firmware contained in IEDs to delay repair attempts.

Figure 3 shows the attack graph representation of the tripping circuit breakers attack. The attacker must compromise protection IEDs in order to trip circuit breakers. In order to do so, the attacker needs to first compromise the gateway and the HMI for gaining access to protection IEDs. For each subsystem, the attacker may be detected at the last step of the attack using IDS_A_1 and IDS_B_1, respectively. In Figure 3, the attacker needs to exploit four different vulnerabilities for each subsystem. On the other hand, to compromise the whole system, the attacker needs six different vulnerabilities (note that the same version number of both protection IEDs, A7, and B7, indicate these are identically configured), so the FoS (Factor of Security) in this scenario can be calculated as follows.

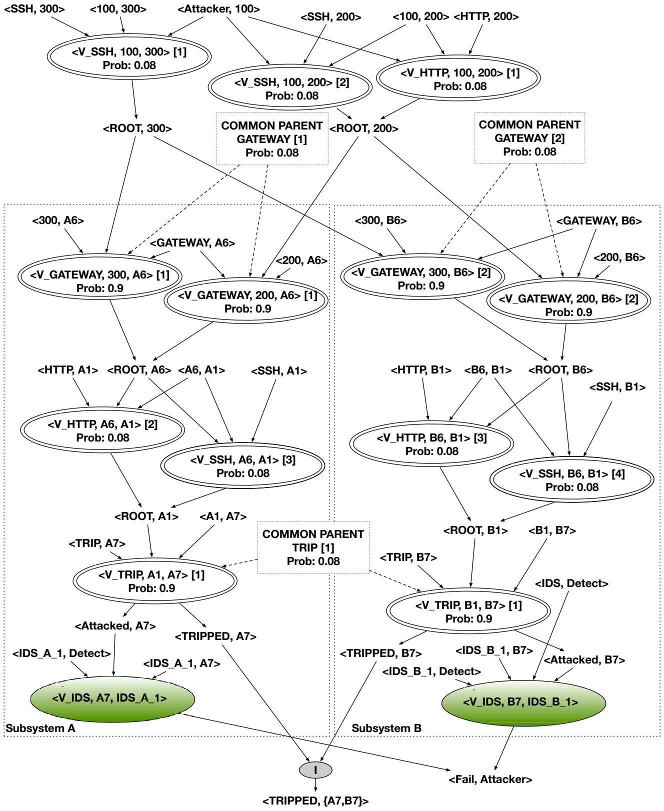


Fig. 3: Attack Graph For Tripping Circuit Breakers

$$FoS = \frac{6}{max(\{4,4\})} = 1.5$$

For the calculation of the PFoS (Probabilistic Factor of Security), we perform Bayesian inference on the goal conditions of subsystems, $\langle TRIPPED, A7\rangle$ and $\langle TRIPPED, B7\rangle$, and on the goal condition of the whole system, $\langle TRIPPED, \{A7, B7\}\rangle$. Probabilities for those nodes can be calculated as follows.

- Pr($\langle TRIPPED, A7\rangle$) = 0.00003544017
- Pr($\langle TRIPPED, B7\rangle$) = 0.00003544017
- Pr($\langle TRIPPED, \{A7, B7\}\rangle$) = 0.000000007

By taking those probabilities into account, PFoS can be calculated as:

$$\begin{aligned} L0 &\leftarrow log_{0.08}(0.000000007) = 7.434431 \\ L1 &\leftarrow log_{0.08}(0.00003544017) = 4.057310 \\ L2 &\leftarrow log_{0.08}(0.00003544017) = 4.057310 \\ PFoS &= \frac{L0}{max(L1, L2)} = 1.832354 \end{aligned}$$

Observation: Comparing those two attack scenarios, we can observe that, the FoS metrics yield different values for different attack scenarios even though those are both with respect to the same underlying substation. In practice, the smart grid operator will need to assign weights to those results to reflect the relative importance of those different threats, and

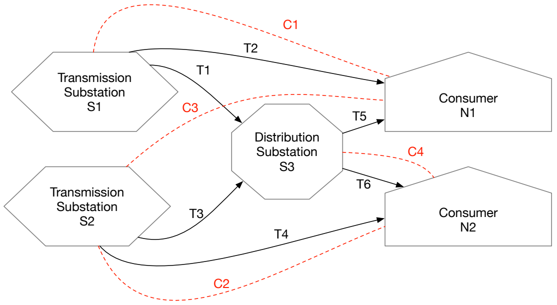


Fig. 4: Graphical Representations of the Smart Grid Transmission and Communication Networks [45]

aggregate the weighted results to evaluate the overall security effectiveness of the design. Also note that, the existence of IDSs does not affect FoS since FoS only depends on the shortest attack path, which would not include an IDS as it will cause the attack to fail. On the other hand, PFoS may be affected by IDSs since PFoS consider all attack paths, and an IDS may cause some attack paths to diverge to the failure nodes and hence reduce the probability of the attack.

B. Attack Scenarios in the Smart Grid Distribution Domain

1) Cascading Link Failure Analysis: The Cascading Link Failure Analysis is introduced in [45]. In this attack scenario, the smart grid network is modeled as a directed graph where the nodes include producer nodes (power generators), intermediate nodes (substations) and consumer nodes (end users), and the edges represent power and communication lines. The goal of attackers is to cause as much power loss as possible by attacking minimal number of transmission and communication lines. If attackers disconnect all incoming power or communication lines to a consumer node, this will cause a blackout at the consumer node. Figure 4 shows a smart grid network which consists of a transmission network and a communication network. In this system, $N1$ and $N2$ are consumer nodes, $S1$ and $S2$ are transmission substations, $S3$ is a distribution substation, $T1$, $T2$, $\cdots$, $T6$ are transmission lines. $C1$, $C2$, $C3$, and $C4$ are communication lines. Assuming $S1$ and $S2$ are secure and cannot be attacked, in order to cause a blackout in the area $N1$, attackers could choose to compromise any of the following combinations, $T2$ and $T5$, $C1$ and $C3$, or both.

In Figure 5, the attacker needs to follow one of the three paths to compromise each subsystem. Among those paths, the shortest path is the path containing two known vulnerabilities (CVE-2012-1442, CVE-2012-0022). Therefore, the attacker can trip $T2\_1$ and $T5\_1$ to cause a blackout in the area $N1\_1$. The $k0d$ value for the shortest path can be calculated as follows.

$$\begin{aligned} k0d\ (T2\_1\ \rightarrow\ T5\_1, \langle Blackout, N1\_1\rangle) \\ = \log_{0.08}(0.43) + \log_{0.08}(0.5) \\ = 0.3341 + 0.2744 = 0.6095 \end{aligned}$$

Similarly, the same two known vulnerabilities can be used to compromise the second subsystem and the $k0d$ value can be calculated as $k0d\ (T2\_2\ \rightarrow\ T5\_2, \langle Blackout, N1\_2\rangle) = 0.6095$.

For the whole system, the attacker can use the same two known vulnerabilities to compromise both subsystems and reach the goal condition "$\langle Blackout, \{N1\_1, N1\_2\}\rangle$". Therefore, the $k0d$ value for the whole system can be calculated as: $AL\ (T2\_1\ \rightarrow\ T5\_1\ \rightarrow\ T2\_2\ \rightarrow\ T5\_2, \langle Blackout, 0\rangle) = 0.6095$

By taking those into account, the FoS value can be calculated as follows.

$$FoS\ =\ \frac{0.6095}{max(0.6095, 0.6095)}\ =\ 1.0$$

For the PFoS metric, we perform Bayesian inference on subsystem goal conditions, which are "$\langle Blackout, N1\_1\rangle$" and "$\langle Blackout, N1\_2\rangle$", and the goal condition of the whole system and the probability can be calculated as follows.

- Pr($\langle Blackout, N1\_1\rangle$) = 0.227665
- Pr($\langle Blackout, N1\_2\rangle$) = 0.13325522
- Pr($\langle Blackout, \{N1\_1, N1\_2\}\rangle$) = 0.0082365287

By taking all of those probabilities into account, the PFoS can be calculated as follows.

$$L0 \leftarrow log_{0.08}(0.107674496) = 0.882376$$
$$L1 \leftarrow log_{0.08}(0.13325522) = 0.7979832$$
$$L2 \leftarrow log_{0.08}(0.227665) = 0.585922$$
$$PFoS\ =\ \frac{L0}{max(L1, L2)} \approx 1.105757$$

Observation: It can be seen that, in this special case, the FoS value of 1 indicates that the design of two subsystems provides no advantage in terms of security resilience against attackers who follow the shortest attack paths. On the other hand, the PFoS value indicates a slightly more optimistic scenario in which attackers may not necessarily (be able to) follow the shortest paths, and hence the redundancy still provides a little more security resilience against such attackers. This is also usually (not always) true in general, i.e., the PFoS is slightly more optimistic than FoS since the former is designed to reflect the average case scenario (i.e., attackers may or may not have the skills and resources to take advantage of the shortest paths).

2) Coordinated Attack against Substations and Transmission Lines: Originally, coordinated attack against substations and transmission lines is presented in [64]. In this attack, attackers concurrently target combinations of substations and transmission lines. Assuming that substations $S1$ and $S2$ are secure and cannot be attacked, the attacker has to target $S3$ and transmission line $T2$, and optionally target transmission lines $T1$ and $T5$ in order to cause a blackout in the area $N1$.

Figure 6 demonstrates the attack graph of the coordinated attack against substation S3 and transmission T2. Attackers can attack substations by compromising substation gateways and attack transmission lines by tripping circuit breakers. In Figure 6, the attacker can first trip the circuit breaker, $T2\_1$, and then compromise the gateway of the substation $S3\_1$, which gives the shortest attack path with the least $k0d$ value. Since $T2\_1$ contains a zero-day vulnerability, exploiting it

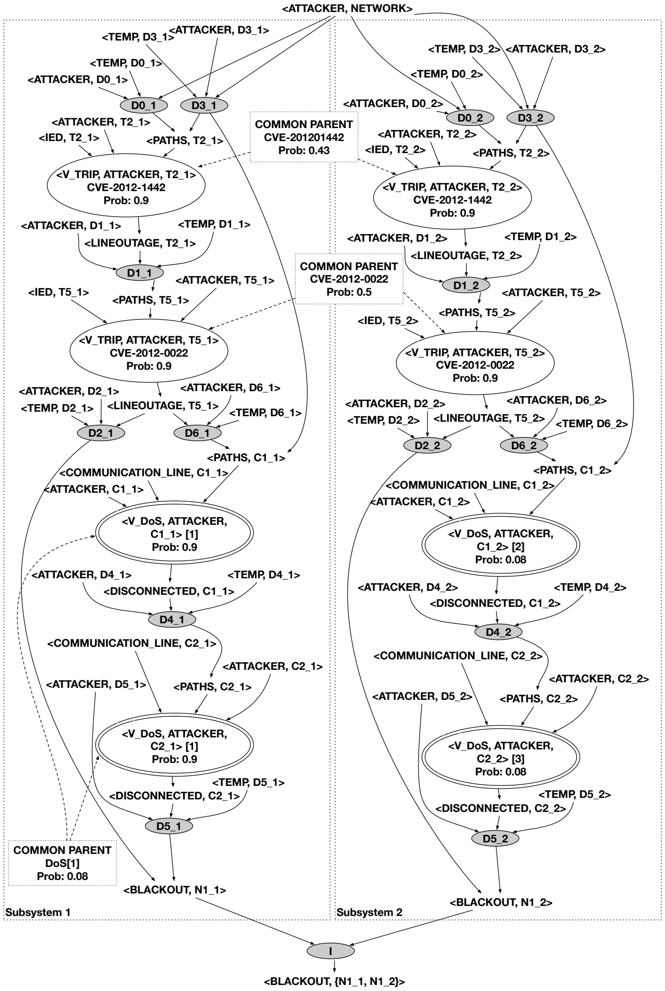


Fig. 5: Attack Graph For Cascading Link Failure Analysis

counts as one toward the $k0d$ value calculation. $S3\_1$ contains a known vulnerability with probability 0.75, so the equivalent $k0d$ value for $S3\_1$ is $log_{0.08}0.75 = 0.1139$. Therefore, the shortest path has a $k0d$ value of 1.1139. A similar calculation applies to the other subsystem and the shortest path also yields a $k0d$ value of 1.1139. For the whole system, the attacker can reuse known vulnerability CVE-2012-0461 for exploiting both $S3\_1$ and $S3\_2$, so he/she needs two zero-day vulnerabilities (those in $T5\_1$ and $T5\_2$) and one known vulnerability (CVE-2012-0461) to compromise the whole system, and the $k0d$ value for the whole system is $2 + 0.1139 = 2.1139$. By taking these into account, the FoS can be calculated as follows.

$$FoS \;=\; \frac{2.1139}{max(1.1139, 1.1139)} \;=\; 1.897747$$

For the calculation of PFoS, we also consider the similarity node in Figure 6 since $T2\_1$ and $T2\_2$ are considered as different but similar IEDs (e.g., different versions). After adding that similarity node, Bayesian inference is performed on goal conditions of subsystems, $\langle BLACKOUT, N1\_1\rangle$ and $\langle BLACKOUT, N1\_2\rangle$, and for the goal condition of the whole system, $\langle BLACKOUT, \{N1\_1, N1\_2\}\rangle$. Probabilities for those nodes are calculated as follows.

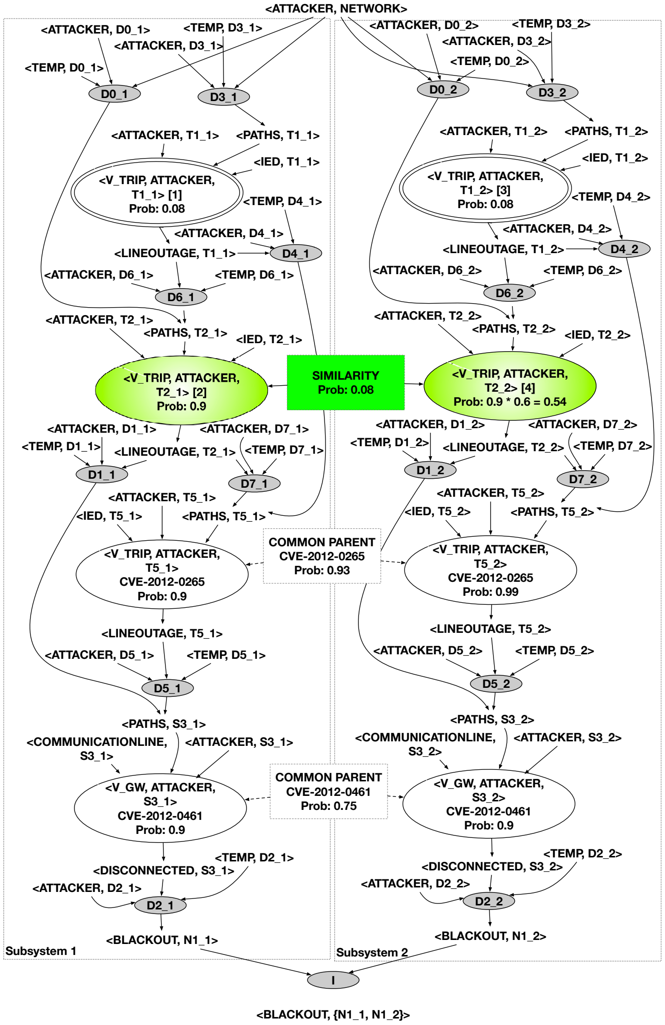


Fig. 6: Attack Graph For Coordinated Attack Against Substations and Transmission Lines

- Pr($\langle BLACKOUT, N1\_1\rangle$) = 0.0603624
- Pr($\langle BLACKOUT, N1\_2\rangle$) = 0.048270
- Pr($\langle BLACKOUT, \{N1\_1, N1\_2\}\rangle$) = 0.018565262

By taking those probabilities into account, the PFoS can be calculated as follows.

$$L0 \leftarrow log_{0.08}(0.018565262) = 1.57834$$
$$L1 \leftarrow log_{0.08}(0.048270) = 1.200027$$
$$L2 \leftarrow log_{0.08}(0.0603624) = 1.1115164$$
$$PFoS \;=\; \frac{L0}{max(L1, L2)} = 1.31525374$$

Observation: It can be seen that, in this special case, the PFoS value is actually smaller than the FoS value, which is opposite to most cases seen above and to the general pattern that PFoS would be slightly more optimistic. Therefore, the behavior of those metrics is not always straightforward, and we will investigate this further in the coming section through simulations.

V. Simulations

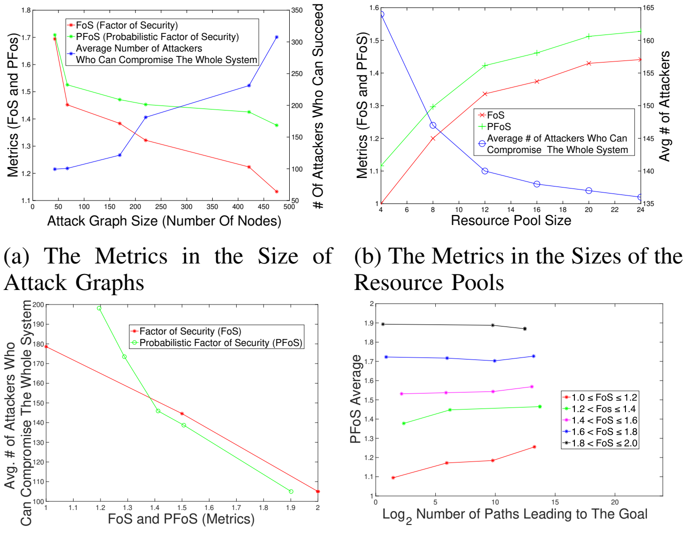
A. Experimental Design

Our simulations are performed on both substation level and smart grid level. We are using IEEE 14 bus [66] for the smart grid level. The IEEE 14 bus does not originally include communication lines, so we make additional effort to add communication lines into IEEE 14 Bus following the literature [31], [45]. In [31], the authors provide communication infrastructure topology for IEEE 14 Bus system and the same communication topology is used in [45]. After adding communication infrastructure to IEEE 14 Bus, we develop attack graphs which include ways in which Bus 5 in IEEE 14 Bus can be attacked in order to cause a blackout, similar to ones in Figures 5 and 6. Energy components and control elements are not considered as parts of the attack graph modeling. Attack graph for the IEEE 14 Bus and other attack graphs shown in the previous section are taken as seed graphs for generating attack graphs. For a given seed graph, a host is added with randomly chosen set of services and random connections are added between the newly added host and existing hosts. Known vulnerabilities are randomly chosen from the vulnerability database, CVE [62]. Zero-day vulnerabilities are assumed to exist in most services. After adding hosts, firewalls and intrusion detection systems are added into attack graphs. Firewalls are added by choosing a random connection condition in the attack graph and putting that connection condition behind a firewall. IDSes are added by choosing a random privilege condition (which is not included in initial conditions) and adding a connection from the chosen random privilege condition to IDS exploit and from IDS exploit to the failure condition.

All simulations are performed on MacOS Mojave 10.14.1 with 2.9 GhZ Core i7 processor and 16 GB RAM. The attack graph generation and FoS calculation are implemented in python 3.6, and the Bayesian inference is based on the automated reasoning tool SamIam [67]. Our experimental setup is summarized in Table II. Section V-B compares the FoS and PFoS in different substation setups. Section V-C studies both metrics with security aspects and Section V-D provides a extensive study with extra security mechanisms. Section V-E studies behavior of metrics with respect to different types of attacks and their combinations.

B. Comparison between FoS and PFoS

In this section, we evaluate the behavior of the metrics based on substation setups. Our first simulation aims to determine how our metrics would behave under different sizes of systems, e.g., when the utility expands their smart grid network or substations. This simulation is based on over 5,000 attack graphs. First, we group attack graphs with similar sizes together and calculate the average FoS and PFoS values for each group. In addition, we generate a set of capabilities (i.e., which vulnerabilities may be exploited) for 500 fictitious attackers where the number of zero-day vulnerabilities exploitable by each attacker follows a normal distribution and the number of known vulnerabilities the attacker can exploit depends on the CVSS score of the known vulnerability (e.g., for a vulnerability with a CVSS score of 9.0, the attacker would be able to exploit it with probability 0.9). We compare the predicted attack resilience results of the FoS metrics to the actual success rate in terms of the number of attackers who can successfully reach the goal condition with their assigned capabilities.



(a) The Metrics in the Size of Attack Graphs

(b) The Metrics in the Sizes of the Resource Pools

(c) The Metrics Applied to IEEE 14 Bus

(d) The Metrics in the Number of Paths

Fig. 7: Simulation Results

Results and Implications: As it can be seen in Figure 7a, as the attack graph size increases, the metrics generally decrease since a larger attack graph would mean more identical components between the subsystems and hence the redundancy becomes less effective in terms of providing security resilience. We can also observe that, in contrast to FoS, PFoS decreases more slowly since it is based on all attack paths. Finally, as metrics decrease, the number of successful attackers increase following a reversed trend, which means the metrics can reflect the expected security effectiveness of the design.

Our second simulation aims to analyze how metrics behave with more diversity available, e.g., when the utility decides to invest in having different types of IEDs, communication equipments and other resources deployed in the same substation. Those different choices of resources are modeled using the version numbers in our attack graphs, as discussed in the previous section, and we will call the collection of such choices as the *resource pool*. We perform simulations by varying the size of the resource pools. This simulation is based on 900 attack graphs and the resource pools sizes are $4, 8, 12, 16, 20,$ and 24.

Results and Implications: As it can be seen in Figure 7b, as the resource pool size increases, both metrics generally increase. However, the improvement gradually flattens out as

	Smart Grid	**Substation**
Type of Attacker	Remote attacker who has access to IED controlling transmission lines, communication lines and substation gateways.	Remote attacker who resides in the same network as the substation gateway.
Attack Scenarios	Cascading link failure analysis and coordinated attack against transmission lines and substations.	PTP time delay attack and tripping circuit breakers attack.
Attack Method	Disconnecting transmission lines, disrupting communication lines or compromising substation gateways.	Exploiting vulnerabilities, delaying PTP messages, tripping circuit breakers.
Number of Nodes in Attack Graphs	10-600	10-500
Characterization of The Power Network	IEEE 14 Bus which includes 14 buses, 5 generators, 11 loads, 17 transmission lines, with communication lines added similar to [45]	The power network is not considered.
Deployment of Firewalls and IDS.	Connectivity conditions are chosen randomly before which firewalls are added. IDSes are added as special types of exploits in which the precondition is one of the postconditions gained by the attacker and if the detection succeeds, the attack fails.	Connectivity conditions are chosen randomly before which firewalls are added. IDSes are added as special types of exploits in which the precondition is one of the postconditions gained by the attacker and if the detection succeeds, the attack fails.

TABLE II: Experimental Setup

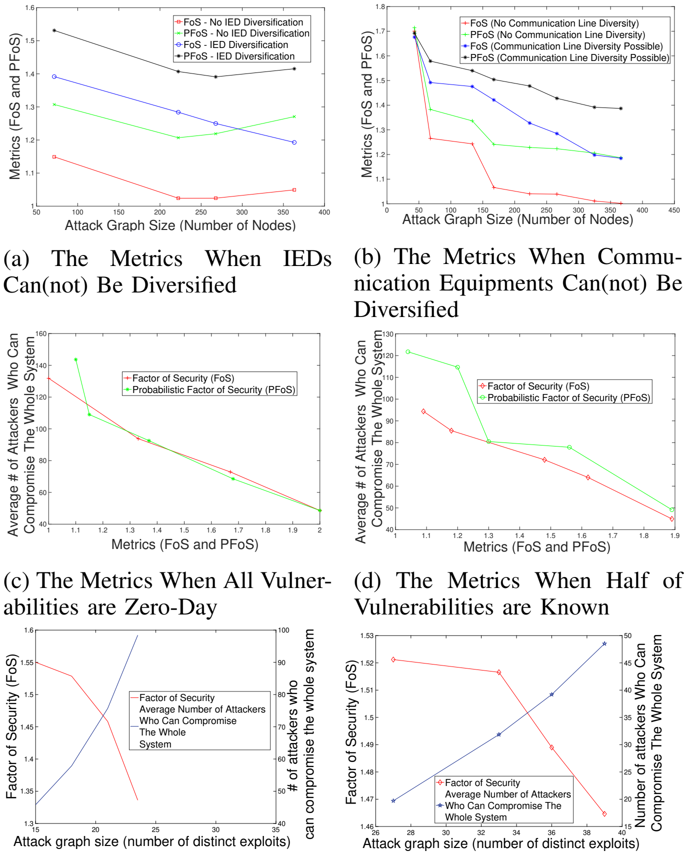
the resource pool size further increases since other factors, such as the shared components between subsystems, become more dominant. Therefore, investing in diversity may improve the security effectiveness to some extent, but ultimately the system design (the topology) becomes the determining factor. Nonetheless, the number of successful attackers still follows a reversed trend as the metrics.

Our third simulation aims to determine how metrics behave at the smart grid level. We developed attack graph models for the IEEE 14 Bus system with communication lines [45], and such attack graphs are taken as seed graphs to generate more attack graphs. We perform simulations to see how the number of successful attackers would change as both metrics increase.

Results and Implications: As it can be seen in Figure 7c, in IEEE 14 Bus systems, the number of successful attackers almost decreases linearly in FoS. The FoS also covers the full range of values between 1 and 2. The PFoS only starts from 1.2 and ends around 1.9, and there is a sharper decrease in the number of attackers before the PFoS value of 1.4. The limited range of values for PFoS is mostly due to average nature of PFoS (i.e., no systems could yield a value less than 1.2 when taking into consideration all the attack paths), which also explains the sharper decrease initially in the number of attackers w.r.t. PFoS (i.e., more systems are clustered around the same PFoS values).

Our fourth simulation aims to determine the relationship between FoS and PFoS. We group attack graphs with similar ranges of FoS values and analyze the relationship between their PFoS values and the number of attack paths (since the key difference between FoS and PFoS is the number of paths that is taken into consideration).

Results and Implications: As it can be seen in Figure 7d, for smaller values of FoS (lower curves), PFoS clearly increases in the number of paths. As FoS gets larger, the trend becomes less obvious (i.e., there is no significant difference between FoS and PFoS). This indicates that, for systems with a smaller value of FoS but a larger number of attack paths (which means the system is poorly designed in terms of both security and redundancy), the difference between the two metrics (i.e., PFoS is more optimistic than FoS) becomes more significant, and hence it becomes more important to consider both metrics at the same time. Conversely, for better designed systems with higher FoS values or fewer paths, the two metrics behave similarly and thus one might be enough.



(a) The Metrics When IEDs Can(not) Be Diversified

(b) The Metrics When Communication Equipments Can(not) Be Diversified

(c) The Metrics When All Vulnerabilities are Zero-Day

(d) The Metrics When Half of Vulnerabilities are Known

(e) FoS for PTP Attack in IEC 61850 Substation When the $k0d$ Value is 5 in Each Subsystem

(f) FoS for PTP Attack in IEC 61850 Substation When the $k0d$ Value is 10 in Each Subsystem

Fig. 8: Simulation Results

C. *Metrics vs Security Aspects*

In this section we simulate various security aspects to observe the behavior of FoS and PFoS. One unique aspect of cyber-physical systems like smart grids is that some components may only be available from a small number of manufacturers, and diversifying such components in practice may not be feasible. Therefore, our next two simulations analyze the effect of such components to the security effectiveness of redundant systems. The fifth simulation analyzes how our metrics behave when IEDs cannot be diversified.

Results and Implications: In Figure 8a, we can see that both metrics yield lower values when IEDs cannot be diversified.

While FoS almost linearly decreases in graph sizes when IEDs can be diversified, the decrease flattens at a certain point in the other three cases, since the role of diversity diminishes and other factors such as the topology becomes more dominant.

Our sixth simulation analyzes how metrics behave when communication equipment cannot be diversified. Since communication in smart grid networks or IEC 61850 substations must follow specific protocols, this is a realistic scenario.

Results and Implications: In Figure 8b, as it can be seen, the gap between metric values (with and without diversity) becomes less compared to the previous case (diversification of IEDs). This implies that the diversity of different components in a system may be of different significance w.r.t. the effect on the overall security effectiveness of the redundant design, e.g., diversifying the IEDs may yield more benefit than diversifying the communication equipment.

Our seventh and eight simulations analyze how the percentage of zero-day vulnerabilities to known vulnerabilities affects the metrics. Two experiments are performed where all the vulnerabilities are assumed to be zero-day in the first, and half of the vulnerabilities are zero-day and known, respectively, in the second.

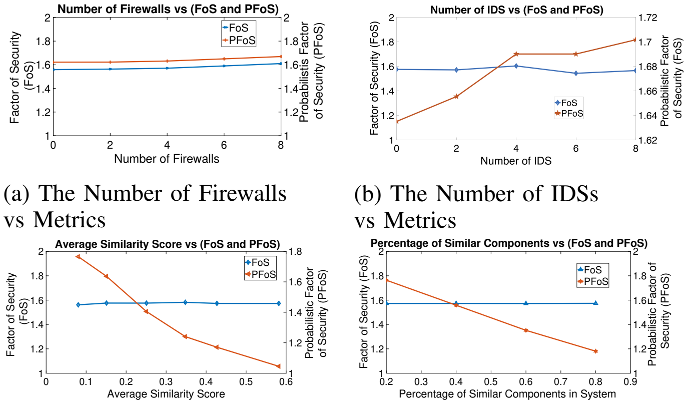
Results and Implications: Figure 8c shows how metrics behave when all vulnerabilities are assumed to be zero-day. As it can be seen, metrics behave similarly when all vulnerabilities are zero-day since all vulnerabilities will be treated the same. Figure 8d shows how metrics behave when half of the vulnerabilities are zero-day and the other half of vulnerabilities are known. In that case, the metrics diverge slightly due to the increasing uncertainty in the CVSS scores of known vulnerabilities.

Our last set of simulations demonstrate how the FoS metric behaves when applied to one specific attack in the IEC 61850 substations. The two simulations are performed by generating attack graph models specifically for the PTP time delay attack-based seed graphs. We focus on the FoS metric, and we fix the $k0d$ value of each subsystem while assuming that all vulnerabilities are zero-day.

Results and Implications: As it can be seen in Figures 8e and 8f, the attack graphs are much smaller in this case since we are considering one specific attack in a substation. We can observe that the results are quite similar to previous cases, i.e., as the size of substations increases, FoS decreases as the number of successful attackers follows a reversed trend. Also, although larger substations may yield larger $k0d$ values, the size does not have as significant effects on the FoS values. In conclusion, the metrics can be applied w.r.t. to one attack or multiple attacks, and are applicable to both substations and the distribution domains.

D. Security Mechanisms and Similarity

Our first two simulations aim to study the effect of an increasing number of security mechanisms including firewalls and IDSs on our metrics. In those experiments, we inject firewalls and IDSs at random locations of each subsystem.



(a) The Number of Firewalls vs Metrics

(b) The Number of IDSs vs Metrics

(c) The Average Similarity Score vs Metrics

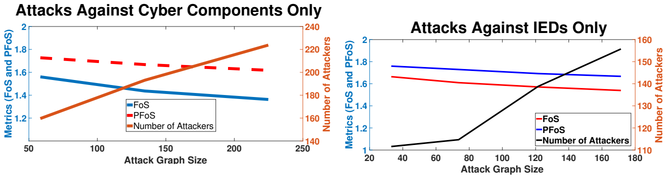
(d) The Percentage of Similar Components vs Metrics

Fig. 9: Security Mechanisms and Similarity

Results and Implications: In Figure 9a, we can see that both metrics increase as the number of firewalls increase, although the trend is slightly different. This is because adding firewalls can potentially increase the length of the shortest path for the whole system more than it does for the shortest path of each subsystem in the case of FoS. For PFoS, adding firewalls increases the length of one or more attack paths. However, as we can see from the results, such an increase is not always significant. In Figure 9b, as it can be seen, adding IDSs does not effect FoS since FoS is only based on the shortest attack path (which will not include detected attacks). On the other hand, PFoS increases as the number of IDSs increase, since the probability that the attacker can reach the final goal or any of subgoals decreases due to the increased detection. This difference also shows the importance of considering both FoS and PFoS in practice.

Our third and fourth simulations study the relationship between component similarity and the metrics. We consider two cases as follows. First, in the case where the similarity between components can be fully quantified or estimated, the average similarity score can be used to represent the relative level of similarity between components. Second, in the case where operators prefer a more simplistic approach of simply regarding some components as “different”, the percentage of similar components can be used. In our simulations, the similarity score of each component is assigned following a uniform distribution between 0.0 and 1.0 and the percentage of similar components is varied from 0.2 to 0.8.

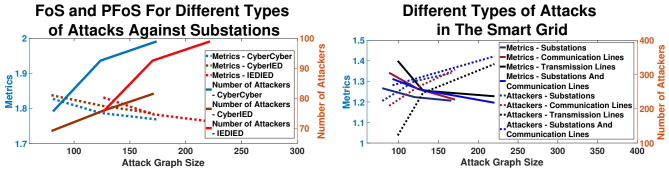
Results and Implications: In Figure 9c, as it can be seen, as the average similarity score increases, FoS is not affected much since the length of the shortest path used in FoS does not consider the similarity between components. On the other hand, PFoS decreases as the average similarity score increases. This is expected since the probability of exploiting the whole system increases with a higher level of similarity between the subsystems’ components. In 9d, it can be seen that the percentage of similar components has no effect on FoS (the reason is similar to the previous case), while it does affect PFoS with a similar trend as in the previous case, which again



(a) Attacks Against Cyber Components

(b) Attacks Against IEDs

Fig. 10: Different Types of Attacks In IEC 61850 Substations



(a) Combining Different Types of Attacks in Substations

(b) Combining Different Types of Attacks in the Smart Grid

Fig. 11: Combining Different Types of Attacks

shows the importance of considering both metrics.

E. Different Types of Attacks

Our first two simulations aim to analyze how metrics change with respect to attacks against cyber components or attacks against IEDs in the substation.

Results and Implications: In Figures 10a and 10b, we can see that metrics and number of attackers who can succeed show a reverse trend. Metric values (FoS and PFoS) are generally larger in the case of attacks against IEDs since attacking IEDs require the attacker to compromise the substation HMI or the workstation. For both attacks against cyber components and IEDs, improving FoS and PFoS improves the security posture of the substation with respect to redundancy. However, for the case of attacks against IEDs, even a small increase in FoS and PFoS causes large decrease in the number of attackers who can compromise both subsystems, compared to attacks against cyber components. This implies that adding a bit diversity in IEDs, such as using different products from the same supplier for an IED as backups, improves the security posture of the substation with respect to redundancy significantly.

Our third and fourth simulations study combinations of different types of attacks in the substation and different types of attacks in the smart grid. For the case of the substation, we combined attacks against cyber components and attacks against IEDs. For the case of the smart grid, we considered four scenarios which are attacking transmission lines only, attacking communication lines only, attacking substations only and attacking both substations and communication lines.

Results and Implications: In Figure 11a, it can be seen that even when different types of attacks are combined, the metrics and number of successful attackers show a reverse trend. In Figure 11b, it can be seen that the metric values for attacks involving transmission lines only is higher since most power systems are designed with N-1 reliability criteria, which means the attacker has to compromise at least two transmission lines in order to compromise the power system. However, the same is not necessarily true for communication lines or substations.

VI. Related Work

The research on analyzing the impact of cyber-physical attacks on smart grid and its components has received significant attention. The reliability impact of four different attack scenarios against substations are analyzed in [11] and it is concluded that there is an opposite trend between reliability and the skill level of attackers. In [32], the authors analyze cyber attack scenarios in integrated wind farm SCADA architecture using the Bayesian attack graph model and indicate that reliability decreases as the frequency of successful attacks and skill levels of attackers increase. Bayesian network model is also used in [29] to quantitatively assess the security risk level of SCADA systems and its effectiveness is demonstrated through simulations. In [68], the authors develop a Bayesian model to evaluate cyber security in nuclear facilities and demonstrate its usefulness through simulations. In [69], the authors model causal relationships between devices in a cyber-physical system using Bayesian model and show its effectiveness for classifying cyber and physical events. In [70], the authors develop a graphical model for representing relationships between vulnerabilities in IoT devices and verify their approach with simulations for different graph sizes. While we also apply similar attack graph and Bayesian network-based techniques, our focus in this paper is different, i.e., on evaluating the security effectiveness of redundancy in smart grid and IEC 61850 substations, which has seen little effort in the literature.

The power system contingency analysis refers to analyzing the impact of failures of different components in the power system and it can be extended to cover contingencies due to cyber attacks in addition to contingencies due to natural faults [13], [14]. In [13], the authors develop a framework for performing impact analysis based on a cyber-physical network to identify critical links, i.e., links which should be the main focus of applying security measures such as adding firewalls or intrusion detection systems. A cyber-physical model for hierarchical control systems is proposed in [71] to evaluate how control commands can influence the power system and it is shown that model-based methods can improve the efficiency of simulation-based methods. Zero-sum Markov games are used to model the interaction between attackers and defenders in [72]; the authors also show how the defender can mislead the attacker through simulations on IEEE 14 Bus system and WECC 9 Bus system. It is shown that attackers can destabilize the power system by controlling multiple circuit breakers and tripping them in a coordinated way in [42]. A multi-stage approach to monitor $n - k$ contingencies is proposed in [73]. A resilience metric is developed and evaluated in [33]. Those works related to contingency analysis help in identifying critical links or components in the power system. Our focus is slightly different although the shortest attack paths used in defining our FoS metric can also be considered as a form of critical links.

The research on redundancy and security in critical control systems has also received significant attention. In [15], the authors propose recovery strategies for restoring controllability in a critical control system following failures in nodes and links. In [16], the authors define control areas which are vulnerable to attacks utilizing dependency graphs. In [74], the authors propose an attack model which involves attacks through vertex removal. In [75], the authors extend the work in [74] by considering combinations of different types of attacks, rather than just considering vertex removal. In [76], the authors propose a policy enforcement system for the heterogeneous smart grid network. In [77], the authors consider restoration of the network using redundant edges. In [78], the authors utilize backup links to ensure that the system is observable when it is attacked using advanced persistent threats. In [79], the authors provide a redundancy based restoration approach by taking the standard IEC 62351 into account. In [80], the authors define a checkpoint based model to produce sufficient data redundancy. This paper differs from those in the sense that we focus on a different aspect which is evaluating the security posture of the system designed as redundant subsystems rather than recovery of the control structure of the system after the system is attacked.

Our work is inspired by the k zero-day safety metric [55] and our Bayesian network-based model is inspired by the existing work on network diversity [54]. However, both works are designed for traditional networks where no redundant subsystems exist. In the context of smart grids, a metric called "exposure" is designed which measures the level of exposure of critical assets [81]; a higher value of exposure means less security for critical assets and the metric is verified by applying it in the context of AMI (Advanced Metering Infrastructure). Metrics measuring the vulnerability of the state estimator to stealthy attacks are proposed in [82] with algorithms for calculating the metrics and verification of their effectiveness. In [83], security metrics are used to quantify the security of each component based on their distance to the critical asset. In [12], several attack graph-based metrics are developed to prioritize assets based on their criticality to the system. The authors in [84] provide a systematic study of model-based and quantitative security metrics. Despite such existing efforts, to the best of our knowledge, little effort exist on quantitatively evaluating the security effectiveness of redundancy in smart grids, which has motivated our work.

VII. Conclusion

In this paper, we have proposed two novel security metrics, namely, the factor of security (FoS) and the probabilistic factor of security (PFoS) to evaluate the security effectiveness of redundant subsystems in smart grids and substations. Specifically, we have provided a concrete design of substation based on IEC 61850 and standard industrial practices. We have adopted the existing factor of safety metric to the context of smart grid security based on the attack graph model to formally define our FoS and PFoS metrics. We have applied the metrics to several attack scenarios in both substations and the smart grid distribution domain. Those attack scenarios have clearly illustrated that our metrics could allow a quantitative understanding about how effective redundant designs are w.r.t. security resilience. We have performed simulations to study how the metrics would behave in different scenarios, and our results demonstrated how the metrics may help answer useful questions about security planning and prioritization in smart grid and substations. The main limitations and our future directions are as follows. First, the metrics do not directly provide a solution for improvement, and hence we plan to develop optimization-based hardening solutions to automatically improve the factor security under given cost constraints. Second, we have focused on external attackers and do not consider inside threats, and we plan to extend our model to cover such threats. Finally, we have relied on simulations and our future work will further evaluate the methodology based on a real testbed.

References

[1] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[2] G. Lu, D. De, and W.-Z. Song, "Smartgridlab: A laboratory-based smart grid testbed," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 143–148, IEEE, 2010.

[3] "Attack on Nine Substations Could Take Down U.S. Grid." "http://spectrum.ieee.org/energywise/energy/the-smarter-grid/attack-on-nine-substations-could-take-down-us-grid". [Online; accessed 23-March-2018].

[4] "Analysis of the cyber attack on the ukrainian power grid." "https://ics.sans.org/media/E-ISAC SANS Ukraine DUC 5.pdf." [Online; accessed 21-March-2017].

[5] I. Standard, "Network engineering guideline for communication networks and systems in substations," tech. rep., IEC 61850-90-4.

[6] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, no. 6, p. 29, 2011.

[7] A. Jaquith, *Security metrics: replacing fear, uncertainty, and doubt*. Pearson Education, 2007.

[8] M. Strobel, N. Wiedermann, and C. Eckert, "Novel weaknesses in iec 62351 protected smart grid control systems," in *Smart Grid Communications (SmartGridComm), 2016 IEEE International Conference on*, pp. 266–270, IEEE, 2016.

[9] T. Phinney, "Iec 62443: Industrial network and system security," *Last accessed July*, vol. 29, 2013.

[10] C. W. Johnson, "Why we cannot (yet) ensure the cybersecurity of safety-critical systems," 2016.

[11] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Power system reliability evaluation with scada cybersecurity considerations," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1707–1721, 2015.

[12] P. S. Patapanchala, C. Huo, R. B. Bobba, and E. Cotilla-Sanchez, "Exploring security metrics for electric grid infrastructures leveraging attack graphs," in *Technologies for Sustainability (SusTech), 2016 IEEE Conference on*, pp. 89–95, IEEE, 2016.

[13] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "Socca: A security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 3–13, 2014.

[14] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2464–2475, 2015.

[15] C. Alcaraz and S. Wolthusen, "Recovery of structural controllability for control systems," in *International Conference on Critical Infrastructure Protection*, pp. 47–63, Springer, 2014.

[16] C. Alcaraz and J. Lopez, "Analysis of requirements for critical control systems," *International journal of critical infrastructure protection*, vol. 5, no. 3-4, pp. 137–145, 2012.

[17] B. Cox, D. Evans, A. Filipi, J. Rowanhill, W. Hu, J. Davidson, J. Knight, A. Nguyen-Tuong, and J. Hiser, “N-variant systems: A secretless framework for security through diversity.,” in *USENIX Security Symposium*, pp. 105–120, 2006.

[18] D. Gao, M. K. Reiter, and D. Song, “Behavioral distance measurement using hidden markov models,” in *International Workshop on Recent Advances in Intrusion Detection*, pp. 19–40, Springer, 2006.

[19] O. Duman, M. Zhang, L. Wang, and M. Debbabi, “Measuring the security posture of iec 61850 substations with redundancy against zero day attacks,” in *SmartGridComm 2017 IEEE International Conference on Smart Grid Communications*, 2017.

[20] “Substation Automation Solutions SAS 600 Series.” http://new.abb.com/docs/librariesprovider101/default-document-library/1kha001069-sen-substation-automation-solutions-sas-600-series.pdf. [Online; accessed 21-March-2017].

[21] “Synchrophasor FAQs.” https://cdn.selinc.com/assets/Literature/Product%20Literature/Flyers/Synchro_FAQs_LM00064-1.pdf?v=20170117-125152. [Online; accessed 21-March-2017].

[22] “IEC61850 Smart Substation.” http://archive.rtcmagazine.com/articles/view/102190. [Online; accessed 21-March-2017].

[23] Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, and S. Sezer, “Multidimensional intrusion detection system for iec 61850-based scada networks,” *IEEE Transactions on Power Delivery*, vol. 32, no. 2, pp. 1068–1078, 2016.

[24] J. Wang and D. Shi, “Cyber-attacks related to intelligent electronic devices and their countermeasures: A review,” in *2018 53rd International Universities Power Engineering Conference (UPEC)*, pp. 1–6, IEEE, 2018.

[25] E. D. Knapp and R. Samani, *Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure*. Newnes, 2013.

[26] “DS Agile Substation Gateway .” https://www.gegridsolutions.com/multilin/energy/catalog/dsagile_substation_gateway.htm. [Online; accessed 23-January-2019].

[27] “HMI.” http://www.subnet.com/resources/dictionary/HMI.aspx. [Online; accessed 9-February-2020].

[28] B. Moussa, M. Debbabi, and C. Assi, “A detection and mitigation model for ptp delay attack in an iec 61850 substation,” *IEEE Transactions on Smart Grid*, 2016.

[29] K. Huang, C. Zhou, Y.-C. Tian, W. Tu, and Y. Peng, “Application of bayesian network to data-driven cyber-security risk assessment in scada networks,” in *Telecommunication Networks and Applications Conference (ITNAC), 2017 27th International*, pp. 1–6, IEEE, 2017.

[30] A. Ashok, M. Govindarasu, and V. Ajjarapu, “Online detection of stealthy false data injection attacks in power system state estimation,” *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1636–1646, 2016.

[31] Y. Wu, L. Nordström, and D. E. Bakken, “Effects of bursty event traffic on synchrophasor delays in ieee c37. 118, iec61850, and iec60870,” in *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*, pp. 478–484, IEEE, 2015.

[32] Y. Zhang, Y. Xiang, and L. Wang, “Power system reliability assessment incorporating cyber attacks against wind farm energy management systems,” *IEEE transactions on smart grid*, vol. 8, no. 5, pp. 2343–2357, 2017.

[33] A. Clark and S. Zonouz, “Cyber-physical resilience: Definition and assessment metric,” *IEEE Transactions on Smart Grid*, 2017.

[34] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, “Time synchronization attack in smart grid: Impact and analysis,” *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87–98, 2013.

[35] D.-Y. Yu, A. Ranganathan, T. Locher, S. Capkun, and D. Basin, “Short paper: detection of gps spoofing attacks in power grids,” in *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks*, pp. 99–104, ACM, 2014.

[36] J. Northcote-Green and R. G. Wilson, *Control and automation of electrical power distribution systems*. CRC press, 2017.

[37] Y. Liu, R. Zivanovic, S. Al-Sarawi, C. Marinescu, and R. Cochran, “A synchronized event logger for substation topology processing,” in *2009 Australasian Universities Power Engineering Conference*, pp. 1–6, IEEE, 2009.

[38] “Protection & Control Relay (IED).” http://www02.abb.com/global/seitp/seitp202.nsf/0/137e4d13c980a910c1257e6700337741/$file/Protection+Control+IED-+Ustika.pdf. [Online; accessed 9-February-2020].

[39] “SYNCHROPHASORS.” https://selinc.com/solutions/synchrophasors/. [Online; accessed 9-February-2020].

[40] P. Castello, C. Muscas, P. A. Pegoraro, and S. Sulis, “Active phasor data concentrator performing adaptive management of latency,” *Sustainable Energy, Grids and Networks*, vol. 16, pp. 270–277, 2018.

[41] “Voltage Transformer.” https://www.globalspec.com/learnmore/electrical_electronic_components/transformers/voltage_transformers. [Online; accessed 23-January-2019].

[42] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, “A coordinated multi-switch attack for cascading failures in smart grid,” *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1183–1195, 2014.

[43] “Current Transformer .” https://www.electronics-tutorials.ws/transformer/current-transformer.html. [Online; accessed 23-January-2019].

[44] “Circuit Breaker .” http://www.subnet.com/resources/dictionary/Circuit-Breaker.aspx. [Online; accessed 23-January-2019].

[45] P. Akaber, B. Moussa, M. Debbabi, and C. Assi, “Cascading link failure analysis in interdependent networks for maximal outages in smart grid,” in *Smart Grid Communications (SmartGridComm), 2016 IEEE International Conference on*, pp. 429–434, IEEE, 2016.

[46] “IEC 61850 Stand Alone Merging Units .” https://www.arteche.com/en/iec-61850-stand-alone-merging-unit-proccess-bus. [Online; accessed 9-February-2020].

[47] D.-T. May and M. Massoud, “On the relation between the factor of safety and reliability,” *ASME Journal ofEngineering for Industry*, pp. 852–857, 1974.

[48] L. Bilge and T. Dumitraş, “Before we knew it: an empirical study of zero-day attacks in the real world,” in *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 833–844, 2012.

[49] “CVE-2010-1151 Detail.” https://nvd.nist.gov/vuln/detail/CVE-2010-1151. [Online; accessed 9-February-2020].

[50] P. Ammann, D. Wijesekera, and S. Kaushik, “Scalable, graph-based network vulnerability analysis,” in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 217–224, ACM, 2002.

[51] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, “Automated generation and analysis of attack graphs,” in *Security and privacy, 2002. Proceedings. 2002 IEEE Symposium on*, pp. 273–284, IEEE, 2002.

[52] K. Kaynar, “A taxonomy for attack graph generation and usage in network security,” *Journal of Information Security and Applications*, vol. 29, pp. 27–56, 2016.

[53] X. Ou, S. Govindavajhala, and A. W. Appel, “Mulval: A logic-based network security analyzer.,” in *USENIX security symposium*, vol. 8, pp. 113–128, Baltimore, MD, 2005.

[54] M. Zhang, L. Wang, S. Jajodia, A. Singhal, and M. Albanese, “Network diversity: a security metric for evaluating the resilience of networks against zero-day attacks,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 1071–1086, 2016.

[55] L. Wang, S. Jajodia, A. Singhal, P. Cheng, and S. Noel, “k-zero day safety: A network security metric for measuring the risk of unknown vulnerabilities,” *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 1, pp. 30–44, 2014.

[56] “Apache HTTP Server Project.” https://httpd.apache.org/. [Online; accessed 17-August-2019].

[57] “Microsoft IIS.” https://www.iis.net/. [Online; accessed 17-August-2019].

[58] “Circl CVE Search.” https://cve.circl.lu/. [Online; accessed 17-August-2019].

[59] P. Giannopoulos and R. C. Veltkamp, “A pseudo-metric for weighted point sets,” in *European Conference on Computer Vision*, pp. 715–730, Springer, 2002.

[60] W. Nzoukou, L. Wang, S. Jajodia, and A. Singhal, “A unified framework for measuring a network’s mean time-to-compromise,” in *Reliable Distributed Systems (SRDS), 2013 IEEE 32nd International Symposium on*, pp. 215–224, IEEE, 2013.

[61] “Cvss v2 calculator.” ’https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator” [Online; accessed 07-March-2018].

[62] “CVE Details.” https://www.cvedetails.com/. [Online; accessed 14-July-2019].

[63] P. Mell, K. Scarfone, and S. Romanosky, “Common vulnerability scoring system,” *IEEE Security & Privacy*, vol. 4, no. 6, pp. 85–89, 2006.

[64] Y. Zhu, J. Yan, Y. Tang, Y. L. Sun, and H. He, “Coordinated attacks against substations and transmission lines in power grids,” in *Global*

Communications Conference (GLOBECOM), 2014 IEEE, pp. 655–661, IEEE, 2014.

[65] "The 2003 Northeast Blackout–Five Years Later." "https://www.scientificamerican.com/article/2003-blackout-five-years-later/". [Online; accessed 13-April-2017].

[66] "IEEE 14-Bus System." https://icseg.iti.illinois.edu/ieee-14-bus-system/. [Online; accessed 9-February-2020].

[67] "SamIam." "http://reasoning.cs.ucla.edu/samiam/". [Online; accessed 23-March-2018].

[68] J. Shin, H. Son, G. Heo, *et al.*, "Development of a cyber security risk model using bayesian networks," *Reliability Engineering & System Safety*, vol. 134, pp. 208–217, 2015.

[69] S. Pan, T. H. Morris, U. Adhikari, and V. Madani, "Causal event graphs cyber-physical system intrusion detection system," in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, p. 40, ACM, 2013.

[70] G. George and S. M. Thampi, "A graph-based security framework for securing industrial iot networks from vulnerability exploitations," *IEEE Access*, vol. 6, pp. 43586–43601, 2018.

[71] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2375–2385, 2015.

[72] C. Y. Ma, D. K. Yau, X. Lou, and N. S. Rao, "Markov game analysis for attack-defense of power networks under possible misinformation," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1676–1686, 2013.

[73] L. Che, X. Liu, and Z. Li, "Screening hidden nk line contingencies in smart grids using a multi-stage model," *IEEE Transactions on Smart Grid*, 2017.

[74] C. Alcaraz, E. E. Miciolino, and S. Wolthusen, "Structural controllability of networks for non-interactive adversarial vertex removal," in *International Workshop on Critical Information Infrastructures Security*, pp. 120–132, Springer, 2013.

[75] C. Alcaraz, E. E. Miciolino, and S. Wolthusen, "Multi-round attacks on structural controllability properties for non-complete random graphs," in *Information Security*, pp. 140–151, Springer, 2015.

[76] C. Alcaraz, J. Lopez, and S. Wolthusen, "Policy enforcement system for secure interoperable control in distributed smart grid systems," *Journal of Network and Computer Applications*, vol. 59, pp. 301–314, 2016.

[77] C. Alcaraz and J. Lopez, "Safeguarding structural controllability in cyber-physical control systems," in *European Symposium on Research in Computer Security*, pp. 471–489, Springer, 2016.

[78] J. E. Rubio, C. Alcaraz, and J. Lopez, "Preventing advanced persistent threats in complex control networks," in *European Symposium on Research in Computer Security*, pp. 402–418, Springer, 2017.

[79] C. Alcaraz, J. Lopez, and K.-K. R. Choo, "Resilient interconnection in cyber-physical control systems," *Computers & Security*, vol. 71, pp. 2–14, 2017.

[80] C. Alcaraz and J. Lopez, "A cyber-physical systems-based checkpoint model for structural controllability," *IEEE Systems Journal*, vol. 12, no. 4, pp. 3543–3554, 2017.

[81] A. Hahn and M. Govindarasu, "Cyber attack exposure evaluation framework for the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 835–843, 2011.

[82] O. Vuković, K. C. Sou, G. Dán, and H. Sandberg, "Network-layer protection schemes against stealth attacks on state estimators in power systems," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pp. 184–189, IEEE, 2011.

[83] S. Zonouz, A. Houmansadr, and P. Haghani, "Elimet: Security metric elicitation in power grid critical infrastructures by observing system administrators' responsive behavior," in *Dependable Systems and Networks (DSN), 2012 42nd Annual IEEE/IFIP International Conference on*, pp. 1–12, IEEE, 2012.

[84] A. Ramos, M. Lazar, R. Holanda Filho, and J. J. Rodrigues, "Model-based quantitative network security metrics: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2704–2734, 2017.