Measuring the Security Posture of IEC 61850 Substations with Redundancy Against Zero Day Attacks

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

***Abstract*—As one of the most critical components of the smart grid, substations are responsible for distributing the energy to end users. According to the substation automation standard, IEC 61850-90-4, substations contain highly complex and interconnected networks, which are typically designed with redundancy to improve the availability in case of failures. The redundancy usually takes the form of multiple subsystems with identical functionality, such that one failed subsystem would not affect the normal operation of the entire substation. However, we show that such redundant subsystems are not always effective against malicious attacks, because, unlike natural faults, attackers may deliberately target the weakest link, i.e., common vulnerabilities found in multiple subsystems. In this paper, we first present a detailed substation configuration designed based on IEC 61850 and industrial practices. We then devise a novel security metric, namely, the factor of security, to measure the effectiveness of redundant subsystems against unknown zero day attacks. We apply the metric to two concrete attacks scenarios, time delay attack, and the tripping circuit breakers attack. Finally, we evaluate the metric through simulations.**

I. Introduction

Designed for managing existing energy more efficiently, the smart grid plays an important role in addressing the global challenge that the demand for energy is growing faster than the supply of energy [1]. The smart grid is a complex system involving many components for the generation, transmission, and distribution of energy to the end users. Found inside the transmission and distribution domains, substations are responsible for protecting, monitoring and controlling the power system to ensure robust delivery of the generated power to the consumers. From the security point of view, substations are one of the most critical components in a smart grid, as demonstrated in a study by the FERC (Federal Energy Regulatory Commission) which shows that a coordinated attack on just nine substations (out of 55,000 substations) can bring down the entire United States power grid [2]. 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 [3], substations were also among the main targets.

To make things worse, the relatively high level of automation inherent to substations [4] could render them an attractive target for the so-called *zero day attacks*. Zero-day attacks are defined as attacks exploiting unknown vulnerabilities [5]. In fact, zero day attacks are usually behind today's high profile security incidents against critical infrastructures (e.g., the Stuxnet attack [6]). Therefore, protecting substations of a smart grid means more than just patching known vulnerabilities and deploying traditional defense mechanisms (e.g., firewalls, IDS (intrusion detection systems)). Going beyond those to further evaluate the resilience of substations against potential zero day attacks is equally important.

To this end, most existing works are insufficient (a detailed review of the related work will be given in Section VI). Among standardization efforts, IEC (International Electrotechnical Commission) 61850 is a commonly used substation automation standard, which is not designed with security [4]. IEC 62351 is designed to provide security protection over IEC 61850, although it has been criticized for its own limitations [7] and it lacks a concrete methodology for modeling and quantifying security. Existing research includes the study of four specific attack vectors of substations and the application of the mean time to compromise metric [8], the contingency analysis for analyzing impacts of failures and for identifying the critical links [9], [10], and smart grid specific security metrics [11], [12]. However, to the best of our knowledge, there exists little effort on quantifying the effectiveness of redundancy against zero day attacks in smart grid substations.

As described in IEC 61850-90-4 [4], a typical solution to improve the availability of substations is through redundancy, which usually takes the form of multiple subsystems with identical functionality. The assumption is that a failure would be limited to one subsystem and therefore would not affect the normal operation of the entire substation. However, such an assumption is less likely to hold, when it comes to malicious attacks. In fact, experienced attackers, who know the substation configuration and who have necessary skills, would naturally target the weakest link in a system. Based on such a key observation, in this paper, we propose a novel security metric, *the factor of security (FoS)*, to measure how well redundancy is designed in a substation from the security perspective. Specifically, we first present a detailed substation configuration designed based on IEC 61850 and vendor specific requirements in order to facilitate further discussions. We then define the factor of security to measure the effectiveness of redundant subsystems against unknown zero day attacks. To demonstrate the usefulness of the metric, we apply it to two

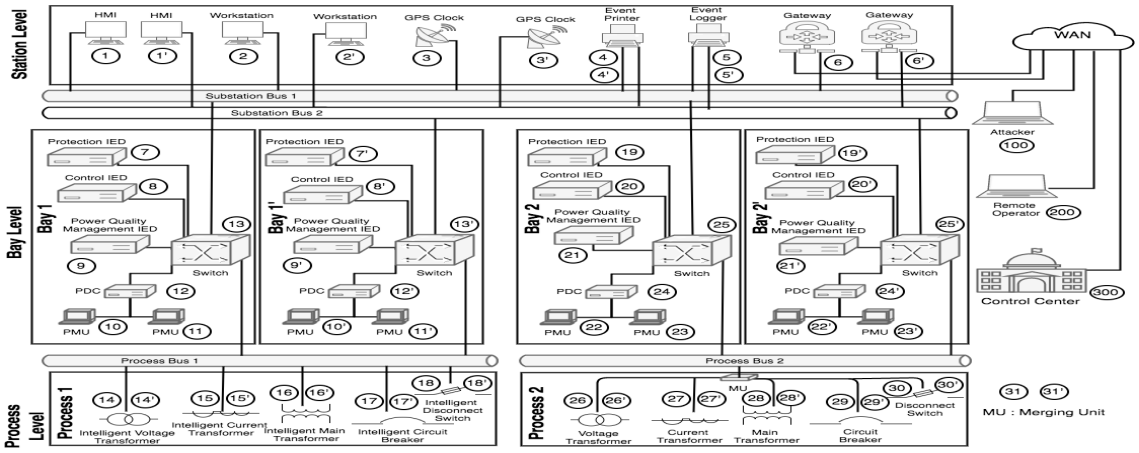


Fig. 1: A Substation with Two Subsystems

concrete attack scenarios, the PTP (Precision Time Protocol) time delay attack [13] and the tripping circuit breakers attack [8]. Finally, we evaluate the metric through simulations. Our contributions are summarized as follows.

- To the best of our knowledge, this is the first effort on formally measuring the effectiveness of redundancy in substations from the security point of view.
- The proposed metric, which is based on well-established techniques such as attack graph modeling and security metrics, provides a practical solution for better understanding the threat of zero day attacks in substations.

This paper is organized as follows: Section II describes a detailed substation design, Section III defines our metric. Section IV applies the metric to two attack scenarios. Section V describes our simulations. Section VI gives a brief review of the related work. Section VII concludes the paper.

II. Designing a Smart Grid Substation based on IEC 61850

To make our discussions more concrete, we present a detailed substation design with redundant subsystems to facilitate further discussions. Although IEC 61850-90-4 provides many sample substation configurations, those are typically overly simplistic and only contain high-level concepts but not concrete details about the hardware or software components, which are essential to the threat modeling process. Therefore, we elaborate a representative substation configuration based on IEC 61850-90-4 and existing industrial practices as follows.

Figure 1 shows a substation with two redundant subsystems, S_1 and S_2. The numbers inside circles ranging from 1 to 31 are components of subsystem S_1 and the numbers from 1' to 31' belong to S_2. A component and its replica are numbered correspondingly, e.g., *node 1'* is the replica of *node 1* (for those which are not replicated, both numbers refer to the same component, e.g., *node 4* and *node 4'*). We assume substations communicate with the control center (*node 300*) through the Wide Area Network (WAN), and the remote operators (*node 200*) also use the WAN to manage substation components 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 [4], a substation can be divided into three levels as detailed in the following:

- **Substation Level:** HMI (Human Machine Interface) is used for monitoring the status of the substation and for sending commands to field devices at the process level (*nodes 1, 1'*). Workstations (*nodes 2, 2'*) are used for automation in the substation. GPS (Global Positioning System) clocks (*nodes 3, 3'*) are used for time synchronization in the substation. An event printer (*nodes 4, 4'*) is used for logging major events. An event logger (*nodes 5, 5'*) is used for logging every event in the substation. All connections to the substation go through substation gateways (*nodes 6, 6'*).
- **Bay Level:** The bay level mostly contains intelligent electronic devices (IED). Bay 1 controls field devices in Process 1, and Bay 2 controls field devices in Process 2. Bay 1' and Bay 2' are replicas of Bay 1 and Bay 2, respectively. 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 7, 7', 19, 19'*) which are used for isolating faults. Control IEDs (*nodes 8, 8', 20, 20'*) are used for managing the power system for efficient usage. In IEC 61850-90-4 [4], there are also IEDs for power quality management, which are included in our design as power quality management IEDs (*nodes 9, 9', 21, 21'*). The PMU (Phasor Measurement Unit)s (*nodes 10, 10', 11, 11', 22, 22', 23, 23'*) and PDC (Phasor Data Concentrator)s (*nodes 12, 12', 24, 24'*) are also contained inside the bays and they are used for obtaining synchronized measurements of voltages and phase angles.
- **Process Level:** The process level contains field devices, e.g., voltage transformers (*nodes 14, 14', 26, 26'*), current transformers (*nodes 15, 15', 27, 27'*), main transformers (*nodes 16, 16', 28, 28'*), circuit breakers (*nodes 17, 17', 29, 29'*), and disconnect switches (*nodes 18, 18', 30, 30'*). All the devices receive commands from IEDs and send measurements to IEDs. Some of those devices (*nodes 26-30, 26'-30'*) must be connected to a merging unit (*nodes*

31, 31') before being connected to the process bus.

To make the design more representative, Figure 1 also reflects many concepts of industrial practices, e.g., SEL [14], Symmetricom [15], ABB [16], etc., as detailed below.

- The design includes two PMUs (*such as nodes 10, 11*) connected to one PDC (*such as node 12*) in each bay, which is based on a similar configuration from SEL [14].
- The design includes ten different field devices, including voltage transformer, current transformer, main transformer, circuit breaker, disconnect switch, and their intelligent counterparts. Intelligent devices (*nodes 14, 14', 15, 15', 16, 16', 17, 17', 18, 18'*) can be directly connected to the process bus. Other devices (*nodes 26, 26', 27, 27', 28, 28', 29, 29', 30, 30'*) need to go through a merging unit (*nodes 31, 31'*) before being connected to the process bus. This is based on a similar configuration given by Symmetricom [15].
- The design includes two subsystems with equivalent functionality, with everything replicated except the event printer (*nodes 4, 4'*) and the event logger (*nodes 5, 5'*). This is based on a similar configuration given by ABB [16] in which the HMI (*nodes 1, 1'*) and the GPS server (*nodes 3, 3'*) are replicated.

In addition to hardware components of the detailed configuration, we also assume following services are running on top of those components. The *GATEWAY* service runs on substation gateways (*nodes 6, 6'*) to prevent unauthorized access to substations. The HMIs and workstations run the *SSH* service for remote maintenance. They also run *HTTP* service for providing a user-friendly interface to substation operators. 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

In this section, we first present the background knowledge for our security metric in Section III-A. We then build the intuitions through the motivating example in Section III-B. Finally, we formally define our metric in Section III-C.

A. Background

Our work is inspired by two well-known metrics, the k-zero day safety in network security [5], and the factor of safety in traditional engineering, as reviewed below.

a) K-zero Day Safety (k0d): The k-zero day safety metric [5] is designed to quantify the risk of zero day attacks in traditional networks. Considering each remotely accessible network service to potentially contain an unknown vulnerability, the metric basically counts the minimum number of distinct 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 exist and be exploitable by the same attacker. In order to calculate k0d for a given network, an attack graph (which is a widely accepted threat model [17]) is developed, and the path with the least number of distinct vulnerabilities, namely, the shortest path, gives the value of k0d. More formally, given a substation with N subsystems, denoted by $S_i (1 \leq i \leq N)$, we use k0d(S_i,μ_i) for the k0d value of the subsystem S_i where the most critical resource is μ_i in S_i. Each subsystem contains one replica of the resource μ and there is only one actively running subsystem where all other subsystems are backups.

b) Factor of Safety: Although not seen in the context of cyber-physical security in the smart grid, the concept of factor of safety is widely used in traditional engineering domains, such as mechanical design, where the factor of safety is the ratio between load carrying capacity (Strength) and the actual load (Stress) for measuring the reliability of a component [18], denoted as $Factor\ of\ Safety = \frac{Strength}{Stress}$. Load carrying capacity is the maximum amount of load that can be carried by the component and the actual load is the expected amount of load to be carried by the component.

B. Motivating Example

Our key idea is to apply the factor of safety concept to subsystems of a substation based on their k-zero day safety values. First, we build intuitions through a motivating example. For the substation depicted in Figure 1, it may seem obvious that, roughly speaking, the factor of safety would be equal to 2, since there exist two subsystems (Strength $= 2$) and only one would be needed for normal operation (Stress $= 1$). Indeed, any fault found in a hardware or software component would most likely be limited to only one of the two subsystems, and hence the substation operator can easily switch 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 an attacker who wishes to cause a blackout to the area and they have identified this substation as their main target. Suppose the attacker compromises a remote operator's machine (*node 200*) through phishing emails leading to the installation of a trojan on that machine. After infecting the substation network using a trojan, the attacker performs reconnaissance, which is basically getting detailed information about the substation configuration. Reconnaissance is used in the case of Ukraine attack [3] . After that, the attacker can use the infected machine as a stepping stone to access the substation HMI in S_1 (*node 1*), assuming S_1 is the actively running subsystem. The attacker (*node 100*) identifies that this HMI is running the HTTP service and subsequently exploits a zero day vulnerability to compromise the HMI. Suppose the substation operators successfully detect the intrusion and switch the actively running subsystem to S_2. However, the HMI in S_2 is running the same version of HTTP service as the HMI in S_1, and therefore the attacker exploits the same zero day vulnerability to compromise both HMIs, and consequently brings down the whole substation and eventually causes a blackout to the area. Clearly, even though the substation has been designed to include two subsystems, an attacker, who has only one HTTP zero day vulnerability in his hand, could compromise both subsystems and hence the

substation. Therefore, from the security perspective, we cannot say the substation offers a factor of safety of 2.

C. The Factor of Security

The above example shows the limitation of adopting an intuitive notion of the factor of safety in evaluating the effectiveness of redundant subsystems. Therefore, we now define a new security metric, *factor of security* (FoS), to allow a formal reasoning about the redundancy of substations in terms of security. Basically, we first define the *strength* of a substation with respect to a given critical asset as the k0d (k-zero day safety, as reviewed in Section III-A) value for the whole system including all replicas of the same asset in all subsystems. This definition basically indicates the level of security (in terms of the least number of distinct zero day vulnerabilities required for compromising all replicas of the critical asset) of the whole system. Also, we define the *stress* of a substation 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 in the substation. Finally, we define the *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. We assume that the attacker compromises the actively running subsystem in the substation and after that, the operator brings up the backup system. After that, the attacker also compromises the backup system. Factor of security is a measure of how effective it is to have those backup systems. It does not take downtime into account.

More formally, the strength of a system S for a given asset μ 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:

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

In our motivating example, the attacker is able to compromise the subsystem following the shortest path (node 100→200→HMI 1 (*node 1*)) in S_1, so k0d(S_1, 1) = 2, and from path (100→200→HMI 1' (*node 1'*)) in S_2, k0d(S_2, 1') = 2. If HMI 1 and HMI 1' run with the same service, the k0d(S, $\{1, 1'\}$) value for the whole substation is 2. The factor of security of this substation is therefore $\frac{2}{2} = 1$. Such a result intuitively says the substation is only as secure as one of its subsystems, which defies the purpose of designing the substation to include two subsystems.

IV. Applying the FoS Metric to Two Concrete Attacks

In this section, we apply our metric to two smart grid specific attacks according to our substation configuration shown in Figure 1. Due to space limitations, we will only show detailed attack graphs for the whole system in each case.

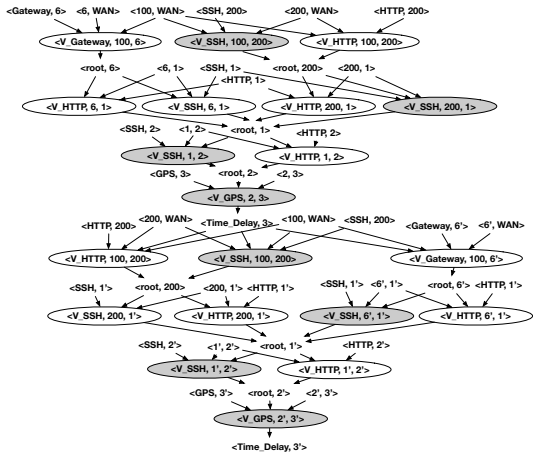
A. PTP Time Delay Attack

The PTP time delay attack aims to delay PTP messages which are used for time synchronization among IEDs in the substation [13]. Time synchronization is critical since the lack of time synchronization can have major consequences such as the control center (*node 300*) making wrong decisions [19]. Given the consequences of lack of time synchronization, PTP time delay attack is used in our paper as a case study to demonstrate the usefulness of our metric.

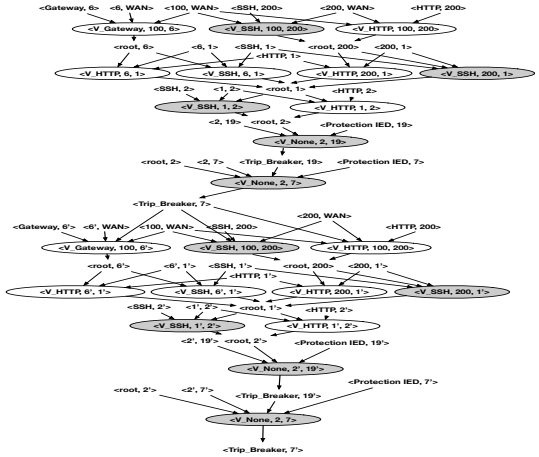
As a protocol used for precise time synchronization in the smart grid [13], PTP requires a master clock, which acts as the main time source, and slave clocks, which get timing information from the master clock. In our model, the GPS clocks (*nodes 3, 3'*) act as PTP masters for each subsystem. In order to attack this protocol, the attacker needs to delay or modify messages used in PTP for time synchronization [13]. An attacker within physical proximity of the substation can use a GPS simulator to spoof GPS messages received by GPS receivers in the substation [20]. However, in our model we do not assume such physical proximity; instead, the attacker is assumed to compromise GPS clocks by remotely accessing to the substation either by compromising substation gateways (*nodes 6, 6'*) or by causing a malware to be installed on the remote operator's machine (*node 200*). In [21], authors proposed a defense mechanism to secure remote control interface placed on substation gateways. However, a zero-day vulnerability [5] in substation gateways can allow an attacker to disable such a defense mechanism.

An attack graph representing PTP time delay attack is given in Figure 2a (where each triple inside an oval indicates an exploit $< vulnerability, source\ host, destination\ host >$ and each pair in clear text indicates either a connectivity relationship such as $< 100, WAN >$, which means the attacker is connected to WAN, or a service running on a host such as $< SSH, 200 >$, which means the remote operator is running SSH service). Exploit nodes in the shortest path are highlighted in gray.

As it can be seen from the attack graph, in order to compromise the GPS clock in the first Subsystem (S_1), the attacker needs one SSH and one GPS vulnerability, so we have $k0d(S_1, 3) = 2$. For the second subsystem (S_2), the attacker also needs one SSH and one GPS vulnerability, so we have $k0d(S_2, 3') = 2$. Even though the substation was designed to include two subsystems, the attacker can bring the whole substation down by using one SSH and one GPS vulnerability. So, the factor of security for the whole substation is $FoS\ (S, \{3, 3'\}) = \frac{2}{2} = 1$. This means that even though the substation was designed to include two different subsystems for redundancy, there is effectively only one subsystem when it is under a PTP time delay attack.



(a) The PTP Time Delay Attack (The Whole System)



(b) The Tripping Circuit Breakers Attack (The Whole System)

Fig. 2: The Attack Graphs for the Two Attacks

B. Tripping Circuit Breakers Attack

Circuit breakers are responsible for protecting transmission lines from damages due to excess current. If a fault is detected on a transmission line, the circuit breaker responsible for that transmission line cuts the flow of the electricity. However, if circuit breakers are tripped by a malicious attacker, this can cause some transmission lines to carry load higher than their capacity and consequently, it may lead to transmission line failures, which may then cause a blackout. For example, transmission line failures were seen in 2003 Northeastern blackout [22]. 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 from the HMI to Protection IEDs [8]. This was seen in the cyber attack against the Ukrainian power grid [3]. In this attack, attackers have tripped circuit breakers by sending remote commands, and they also have changed firmware contained in IEDs to delay repair attempts. This attack shows the importance of protecting substations against tripping circuit breakers attack.

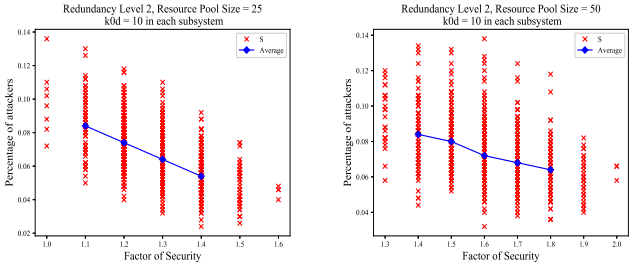
Figure 2b shows the attack graph which represents tripping circuit breakers for the whole system. In order to bring S_1 down, the attacker has to compromise protection IEDs in S_1 (*nodes 7, 19*). After the attacker has compromised the workstation (*node 2*) by using HMI (*node 1*) as the stepping stone, the attacker does not need any additional exploits to compromise protection IEDs (*nodes 7, 19*). This is shown as "None" in the attack graph and those exploits are not counted in calculations of the k0d values. Therefore, the factor of security for the substation is also equal to 1 if protection IEDs are considered as critical resources (μ).

V. Simulation Results

To evaluate the proposed metric, we generate substation configurations similar to the one given in Figure 1 while assigning services to components in a random but realistic fashion. For example, HMIs (*nodes 1, 1'*), workstations (*nodes 2, 2'*) and the remote operator (*node 200*) can include either HTTP, SSH, or both; GPS clocks (*nodes 3, 3'*) can include GPS service; Gateways (*nodes 6, 6'*) can include GATEWAY service, etc. Also, a resource pool including different instances of each service is created from which service instances are randomly selected for assigning to hardware components; this mimics the practice of diversifying services for security based on the fact that different service instances (e.g., IIS and Apache for HTTP service, are less likely to share the same zero day vulnerability than two identical instances would [23]). In practice pool size can be small depending on services and components. Finally, we follow common industrial practices to consider two or three subsystems in our simulations, with one functional subsystem and one or two backups. We perform our simulations on a computer running MacOS 10.12.4 with 16 GB RAM and 2.9 GHz Intel Core i7 CPU.

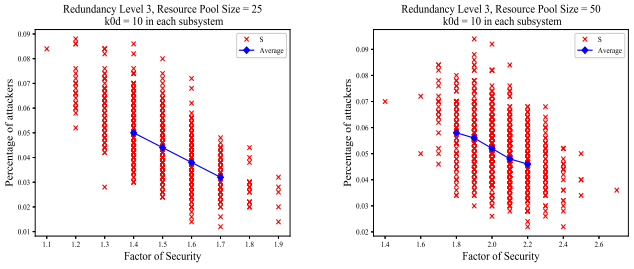
The objective of our first set of simulations is to examine how well the factor of security (FoS) reflects the level of security, when the k0d value is fixed for both subsystems of different substation configurations. Parameters of simulations include the size of the resource pool, the number of subsystems, and the k0d value of each subsystem. For comparison to the FoS values, we simulate attacker capabilities as subsets of service instances which they are assumed to have the skills to compromise, with the level of attackers' capabilities (i.e., the number of service instances they can compromise) following the Gamma distribution [24]. We generate 500 random attackers with different capabilities in each experiment. Finally, with a fixed k0d value for both subsystems, we examine the relationship between the average FoS value and the percentages of attackers who can successfully reach the critical assets, the GPS clocks, in the attack graphs of the substations. We repeat each experiment 1000 times and take the average value.

Results and Implications: Figure 3a and Figure 3b show the FoS versus the percentage of successful attackers (among 500 attackers) for substations with two subsystems, both with a k0d value of 10, and a resource pool size of 25 and 50, respectively. The percentage of attackers, S, is shown as red



(a) Resource Pool Size 25 (b) Resource Pool Size 50

Fig. 3: The FoS vs. the Percentage of Successful Attackers (Two Subsystems)



(a) Resource Pool Size 25 (b) Resource Pool Size 50

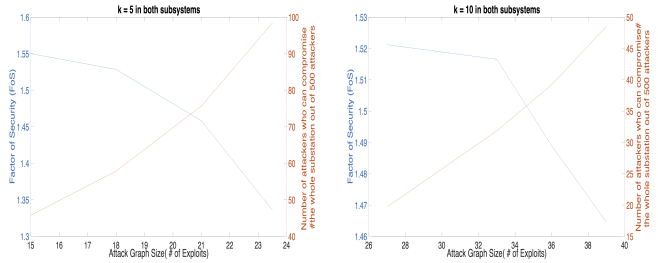
Fig. 4: The FoS vs. the Percentage of Successful Attackers (Three Subsystems)

crosses in the figure and the average is shown as the blue line. From the results, we can observe that, in both cases, the FoS values and the percentage of successful attackers S are roughly inversely proportional, which is expected since a higher FoS value indicates a better configured substation whose redundant subsystems are more resilient to attacks. On the other hand, the different ranges of FoS values ($1.0-1.6$ vs. $1.3-2.0$) in Figure 3a and Figure 3b show that a larger resource pool (i.e., more service instances available) allows higher FoS values.

Figure 4a and Figure 4b show the results for redundancy level 3 (i.e., with three subsystems) with the same resource pool sizes. We can observe that, in contrast to the previous two figures, although the level of redundancy increases by one, the FoS values do not increase as much. In fact, the FoS values only see small increases (from $1.1-1.4$ to $1.4-1.7$ for resource pool size 25, and from $1.4-1.8$ to $1.8-2.2$ for resource pool size 50). Also, for the same FoS values, the percentage of successful attackers remain the same regardless of the redundancy levels. Therefore, we can conclude that, in addition to the redundancy level, the level of diversity available for assigning services to different components also plays a critical role in increasing the FoS values of substations.

The objective of our second set of simulations is to investigate how the FoS values are affected by the size of substations. Here we repeat our experiments 1500 times for k0d = 5 and k0d = 10 for both subsystems, respectively. We first generate substation configurations of different sizes, and we group those configurations with similar sizes of their corresponding attack graphs. We then calculate the FoS values and the percentage of successful attackers.

Results and Implications: Figure 5 shows both the FoS values (the left Y-axis) and the percentage of attackers (the right Y-axis) in the sizes of attack graphs. We show the simulation results in which both subsystems have k0d = 5 and



(a) K = 5 in both subsystems (b) K = 10 in both subsystems

Fig. 5: The FoS and the Percentage of Successful Attackers in the Sizes of Attack Graphs

k0d = 10, respectively. We can observe that, as the sizes of substations increase, the factor of security (FoS) decreases, as the relative amount of diversity decreases under a fixed resource pool size. Accordingly, the number of successful attackers increases following a similar trend as in previous experiments. By comparing the two figures, we can also observe that, although larger substations are required to yield larger k0d values (hence lower percentages of successful attackers), these do not have a significant effect on the FoS values. Therefore, we can conclude that the proposed FoS metric again closely matches the level of security of substations under fixed k0d values for each subsystem, and for larger substations, a higher level of diversity would be required to achieve the same FoS values of the substations.

VI. Related Work

Research on protecting substations against security attacks has attracted significant attention. The reliability impacts of four different attack scenarios are analyzed in [8] and the authors conclude that as substations are attacked by more skilled attackers, their reliability decreases. The power system contingency analysis is extended to include contingencies due to cyber attacks in [9] and [10]. Critical links are identified as the result of contingency analysis. In contrast to those works, our work focuses on measuring the effectiveness of redundancy in substations with respect to security.

Most existing works on security metrics and risk assessment focus on known vulnerabilities [25], [26]. A few exceptions include the "k zero-day safety" model, which basically counts the minimum number of zero day vulnerabilities required to compromise a network asset [5], and the network diversity model, which formally characterizes the level of diversity in a network [23]. Security metrics are also defined in the context of the smart grid. A metric called *exposure*, which measures how exposed critical assets are to attackers is proposed in [11]. Security metrics to measure the vulnerability of the state estimator to attacks against communication infrastructures is developed in [27]. Security metrics for measuring the vulnerability of the power grid against data integrity and availability attacks are proposed in [28]. Security metric which measures the security of each component according to their distances to critical assets is developed in [12]. Redundancy is used to detect anomalies in [29] by comparing outputs of different replicas in response to the same input and it is shown to

be effective to detect attacks that can not be easily detected including zero day attacks. In our case, only one subsystem is active and after that subsystem is compromised the operator switches the actively running subsystem to one of the backup subsystems. Lastly, the factor of safety is used in the context of the smart grid for analyzing cascading failures [30]. In contrast to those works, our security metric, the factor of security, focuses on a different and novel aspect, i.e., the level of redundancy in substations.

VII. Conclusion

In this paper, we have developed a novel security metric, *factor of security*, for evaluating the effectiveness of redundant subsystems in substations from the security point of view. We have applied the metric to two concrete attack scenarios, and evaluated it through simulations. Our future work will be directed to address several limitations, including an automated hardening approach to improve the factor of security according to the trade-off between security gain and complexity, revising the metric for handling coordinated attacks where two attackers have different skill sets and perform a coordinated attack, a complementary probabilistic approach to model the factor of security for both known and zero-day attacks, developing a realistic cost model of maintaining multiple redundant replicas with different configurations and validating attack graph models used to calculate factor of security.

Acknowledgement

The authors thank the anonymous reviewers for their valuable comments. The research reported in this paper is supported by the NSERC/Hydro-Québec Thales Research Chair in Smart Grid Security.

References

[1] 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.

[2] "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 6-April-2017].

[3] "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].

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

[5] 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.

[6] N. Falliere, L. O. Murchu, and E. Chien, "W32.stuxnet dossier." Symantec Security Response, 2011.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

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

[15] "IEC61850 Smart Substation." https://www.slideshare.net/symmetricomsymm/time-synchronisation. [Online; accessed 21-March-2017].

[16] "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].

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] D. Mashima, P. Gunathilaka, and B. Chen, "An active command mediation approach for securing remote control interface of substations," in *Smart Grid Communications (SmartGridComm), 2016 IEEE International Conference on*, pp. 147–153, IEEE, 2016.

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

[23] 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.

[24] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel, "Time-to-compromise model for cyber risk reduction estimation," in *Quality of Protection*, pp. 49–64, Springer, 2006.

[25] N. Idika and B. Bhargava, "Extending attack graph-based security metrics and aggregating their application," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 75–85, 2012.

[26] L. Wang, A. Singhal, and S. Jajodia, "Toward measuring network security using attack graphs," in *Proceedings of the 2007 ACM workshop on Quality of protection*, pp. 49–54, ACM, 2007.

[27] 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.

[28] K. Pan, A. M. Teixeira, M. Cvetkovic, and P. Palensky, "Combined data integrity and availability attacks on state estimation in cyber-physical power grids," in *Smart Grid Communications (SmartGridComm), 2016 IEEE International Conference on*, pp. 271–277, IEEE, 2016.

[29] R. Venkatakrishnan and M. A. Vouk, "Using redundancy to detect security anomalies: Towards iot security attack detectors: The internet of things (ubiquity symposium)," *Ubiquity*, vol. 2016, pp. 1:1–1:19, Jan. 2016.

[30] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman, "Sensitivity analysis of the power grid vulnerability to large-scale cascading failures," *ACM SIGMETRICS Performance Evaluation Review*, vol. 40, no. 3, pp. 33–37, 2012.