# Tabulating Cybersecurity Solutions for Substations: Towards Pragmatic Design and Planning

Heng Chuan Tan*, Carmen Cheh†, Binbin Chen*, Daisuke Mashima*
*Advanced Digital Sciences Center, Singapore †University of Illinois at Urbana Champaign, USA
Email: {hc.tan,Binbin.chen,Daisuke.m}@adsc-create.edu.sg, cheh2@illinois.edu

***Abstract*—Electric substations play an important role in the proper functioning of power grid systems. Recent incidents such as the Ukraine case have demonstrated the high risk of attacks against substations. A wealth of existing and emerging cyber defense mechanisms have been suggested for protecting substations, each with different defense objectives and using a variety of approaches that have their own strength and weakness. In this paper, we propose a pragmatic framework for reasoning about the different mechanisms by allowing critical comparisons of their features and the planning of their composition. The scope of our framework is general and can cover heterogeneous defense mechanisms, such as software integrity and physical zoning. We define specific criteria in our framework to compare those defense mechanisms in order to generate pragmatic deployment suggestions. We demonstrate the benefits of our framework by conducting a case study inspired by the Ukraine attack.**

## I. Introduction

The substation is an integral part of the Smart Grid (SG), providing seamless power to the end-users. Its main function is to regulate the voltage for transmission and distribution [1]. As the demand for electricity increases, multivendor devices with proprietary protocols have become commonplace in substations. To address the interoperability issues, the IEC 61850 standard has developed a common communication profile for exchanging information across vendors, settings and device types [2]. The result of this standardization is the formulation of abstract data objects that can be mapped to various protocols, such as the Manufacturing Message Specification (MMS), the Generic Object Oriented Substation Event (GOOSE), and the Sampled Measured Values (SMV).

Despite the increased connectivity, the use of IEC 61850 standard has also increased the attack surface of the substation. Recent investigations into the power outage in Ukraine has revealed that the cause of the disruption was actually due to a malware called CrashOverride [3] that has the capability to manipulate devices using the IEC 61850-based protocols. Specifically, attackers can modify the status and sequence numbers in the GOOSE message to cause the circuit breaker to malfunction [4], [5], [6]. Attackers can also desynchronize the networked measurements by attacking the Precision-Time Protocol (PTP) [7]. In addition, implementation attacks such as false injection attacks, hardware Trojans, and logic bombs [8] can also compromise the Intelligent Electronic Device (IED) and Programmable Logic Controller (PLC) at the substation level.

To counter those attacks, many defense solutions have been developed and in some cases, adopted in the SG. These solutions vary from standard IT technologies such as firewalls, intrusion detection system (IDS), and encryption to more sophisticated technology like deception mechanisms. While these solutions are effective, there is no systematic approach to reason about the different solutions and to suggest a strategic combination of those solutions to an SG operator. To fill this gap, we present a pragmatic framework that allows the practitioners to conduct their own assessments and identify the best combination of defense mechanisms that work seamlessly. Specifically, our framework answers the following questions:

- What are the strengths and weaknesses of the defense mechanism from a business and operational perspective?
- What types of assets and which attack phases can the defense mechanism protect?
- Given two defense mechanisms $A$ and $B$, do they complement or oppose each other?

We believe that using our framework can facilitate the decision-making process and allow practitioners to prioritize defenses for quicker deployment.

## II. Related Work

Many frameworks have been proposed to guide the selection of defense mechanisms. In [9], the authors proposed two taxonomies for classifying distributed denial of service (DDoS) attacks and their associated defenses to better understand the threats and the possible DDoS countermeasures. In [10], the authors proposed a taxonomy for describing the semantic attack landscape and used it to evaluate the defense mechanisms to determine their suitability. In [11], the authors applied the cost-benefit analysis to determine the trade-off between the cost of detecting and the cost of responding to intrusions to maximize the Return on Investment (ROI) for IDS deployment. The work in [12] investigated the IDS design for cyber-physical systems based on detection technique and data preprocessing technique to gain insight into the effectiveness of the various techniques. More recently, authors in [13] proposed a new classification of attacks based on different layers of the SG (i.e., systems layer, software layer, and communication layer) to establish a common knowledge base for designing effective countermeasures.

Unfortunately, these taxonomies can only compare specific classes of defense solutions. In contrast, our framework is able to compare general classes of defense and provide suggestions on the composition of solutions to build a defense-in-depth strategy.

TABLE I
QUANTITATIVE SCALES OF MEASUREMENT FOR EACH METRIC

| Cost | | | Intrus-iveness | Exploit-ability | Compat-ibility | Mat-urity | Protection Coverage | | |
|---|---|---|---|---|---|---|---|---|---|
| Deployment | Operating | Maintenance | | | | | Assets types | Attack phases | |
| Low | Low | Low | Low | Easy | Dependency | Immature | Physical devices | Recce | Installation |
| Medium | Medium | Medium | Medium | Moderate | Conflict | Partial | Network access | Weaponize | Command & Control |
| High | High | High | High | Hard | Neutral | Fully | Host data | Delivery | Action on Objective |
| | | | | | | | Network data | Exploitation | |

Note: The values for the cost metric are defined as follows: Low (<USD10,000); Medium (between USD10,000 and USD50,000); High (>USD50,000)

## III. FRAMEWORK DESIGN

Our goal is to design a common set of metrics to evaluate the various defense mechanisms. A key aspect is that the metrics should be flexible and adaptable for most classes of defense solutions. To achieve this goal, we consider several criteria. First, the metric must be easy to understand. Second, the metric should meet our design objective, i.e., for evaluating the suitability of a defense mechanism. Lastly, the metrics should be generic enough to allow cross-comparison between different defense mechanisms. Following these criteria, we define six metrics namely, *Cost, Intrusiveness, Protection Coverage, Exploitability, Compatibility,* and *Maturity in terms of technology* and summarize their quantitative scales of measurement in Table I.

- *Cost* defines the amount of money an organization spends on its defenses in relation to its deployment, operation, and maintenance aspects.
- *Intrusiveness* defines the level of interactivity between a defense mechanism and a host system.
- *Protection coverage* defines the scope of protection that a defense mechanism is intended to provide, and can be divided into two types: asset types and attack phase [1] [14].
- *Exploitability* measures the difficulty of circumventing the defense mechanism.
- *Compatibility* measures the degree of dependency, i.e., how much each defense mechanism supports one another to achieve defense-in-depth protection.
- *Maturity* of the defense mechanisms defines the readiness level of the technology.

## IV. REVIEW OF DEFENSE MECHANISMS

In this section, we use the framework to review the state-of-art defense mechanisms and summarize their strengths and weaknesses in Table III.

### A. Zoning

Zoning divides the system into different protection zones to isolate and prevent failures from propagating to other parts of the system and can be classified into two types: (1) physical zoning, and (2) network zoning. In physical zoning, the power grid is divided into different physical zones (e.g., transformer zone, busbar zone, feeder zone) where each zone is protected by an overcurrent relay [15], [16]. In network zoning, the grid is divided into different communication zones (e.g. control zone, corporate zone, and demilitarized zone), each protected by firewalls and data diodes [17], [18]. A firewall is a configurable device that only allows authorized traffic to access the protected network. A data diode is a hardware that limits communication flow in only one direction to control the flow of sensitive data in and out of an organization [19].

*Discussion:* Physical and network zoning has **low** deployment, operating, and maintenance costs. Zoning is relatively easy to set up although in the case of firewalls, some customization may be required to adapt commercial firewalls to recognize substation protocol traffic. We also note that the setup for data diodes is irreversible after installment. After deployment, zoning does not interfere with system operation and thus, has **low** intrusiveness. Physical zoning protects the **physical devices** against the last attack phase **actions on objective** whereas network zoning protects **network access** from being compromised by the attacker in the **delivery** and **reconnaissance** attack phase. Although both physical and network zoning are **fully** mature, physical zoning can be **moderate**ly subverted by attackers since it only protects against the last attack phase. Network zoning is **easy** to subvert if the firewall is compromised or if there are loopholes in the firewall rules.

### B. Secure Policies and Protocols (as covered in IEC 62351)

The IEC 62351 standard proposed by WG15 of TC57 is the current standard for providing data and communication security in the substations. Cryptography and key management are two key aspects mentioned in this 13-part document. It was developed to address the security issues of the TC57 protocols, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, IEC 61970 and the IEC 61968 series [20]. The first two parts of the standard introduce various aspects of security as applied to power system operations. Parts 3-6 specify security requirements for the different TC57 communication profiles, while parts 7-13 provide guidelines on the management of information systems, including access control and key management. Table II summarizes the various parts of the standard, focusing in part on the security goals.

[1]Reconnaissance refers to the act of gathering information in order to identify vulnerabilities in the target network. Weaponization refers to a process of coupling a exploit with a backdoor to make a deliverable payload. Delivery refers to the process of delivering the malicious payload into the system. Exploitation refers to the process of triggering the payload to exploit the vulnerability. Installation refers to the process of installing a backdoor that an attacker can use. Command and control refers to the process of establishing a control channel for persistant access to the system. Actions on objectives refers to a successful completion of an attack on the system.

TABLE II
OVERVIEW OF THE IEC 62351 STANDARD

| Description | Mechanism | C | I | Au | A | NR | Az |
|---|---|---|---|---|---|---|---|
| Part 3 - Security for any TCP/IP-based profiles | TLS | ✓ | ✓ | ✓ | - | - | - |
| Part 4 - Security for MMS-based profiles | Transport (T)-Profile - TLS | ✓ | ✓ | ✓ | - | - | - |
| | Application (A)-Profile - Peer authentication using certificate | - | - | ✓ | - | ✓ | - |
| Part 5 - Security for IEC 60870-5 and derivatives such as DNP-3 | Serial version - Challenge-response protocol | - | ✓ | ✓ | - | - | - |
| | Networked version - TLS with encryption only | ✓ | ✓ | - | - | - | - |
| Part 6 - Security for IEC 61850 profiles | GOOSE and SV - Digital signature | - | ✓ | ✓ | - | - | - |
| | MMS - TLS and Peer authentication using certificate | ✓ | ✓ | ✓ | - | ✓ | - |
| Part 8 - Access control in power systems | Role-Based Access Control (RBAC) | - | - | - | - | - | ✓ |
| Part 9 - Key management for power systems | Certificate-based PKI | End-to-End Security | | | | | |

C=Confidentiality; I=Integrity; Au=Authentication; A=Availability; NR=Non-repudiation; Az=Authorization
MMS=Manufacturing Messaging Service; GOOSE=Generic Object Oriented Substation Events; SV=Sampled Value

*Discussion:* Enforcing IEC 62351 has **high** deployment, operating, and maintenance costs due to the high management costs of deploying a Public Key Infrastructure (PKI). IEC 62351 is **high**ly intrusive to the system because the cryptographic primitives operate on the operational data, but if deployed correctly, the standard is able to protect the **network** and **host data** from being read and modified during the **reconnaissance and delivery** attack phases. The standard is **partial**ly mature and it is very **hard** to be subverted by attackers due to the strong mathematical assumptions. However, the standard does not address implementation attacks (e.g., false injection attacks, hardware Trojans, and logic bombs [8]) on the embedded systems [15] such as IED and PLC.

### C. Intrusion Detection System (IDS)

IDS is a hardware or software application that monitors the system's network and/or hosts to detect any malicious activity by using: (1) signature-based methods where system activity is checked against a database of known attack patterns, or (2) anomaly-based methods where system activity is checked against a "normal" baseline model for any deviations. Anomaly-based methods can be further divided into statistical-based, machine-learning based, and physics-based.

Statistical-based IDS builds a baseline model of the system by applying statistical analysis (e.g., mean, standard deviation) to a small sample of system activity [21], [22], [23]. On the other hand, machine-learning based IDS uses learning algorithms that can autonomously integrate data to build a baseline model of the system activity. One key difference between the machine-learning based and statistical-based IDS is that machine-learning is more focused on data analysis that enables the IDS to self-learn and to perform prediction. For physics-based IDS, a model describing the physical properties or physical state of the system is derived [24], [25], [26]. The sensor data collected in real time is then compared to the model by performing a state estimation of the physical system or utilized for power-flow simulation. However, such advanced detection method incurs latency. In order to integrate it, we can rely on command-delaying technology proposed in [27].

*Discussion:* All the IDSes have **low** intrusiveness to the system because they passively collect data and only raise alarms to the operator. Signature-based IDS has a **low** deployment cost but a **medium** operating and maintenance cost because of the need to update the signature database regularly, and as the size of the database increases, the processing load also increases. All the anomaly-based IDSes have **low** operating cost because they do not need to be updated. Of the anomaly-based IDSes, physics-based IDSes has the **high**est deployment and maintenance costs, followed by machine-learning based IDS with a **medium** deployment and maintenance cost, and statistical-based IDS with a **low** deployment and maintenance cost. That is because physics-based IDS requires expert knowledge about the system and real-time operational data to build the "physics" model of the system and manual tuning after deployment to ensure its accuracy. Although machine-learning approach requires a large number of training samples to produce meaningful results [28], [29], it only needs to be trained once during the deployment phase followed by periodic retraining during the maintenance phase.

All the IDSes protect the **network data** and the physics-based IDS additionally protects **host data** from being modified by comparing actual sensor measurements to predicted ones produced by the state estimation. All the IDSes protect against the **reconnaissance, delivery, exploitation, installation, command and control, and actions on objective** attack phases. Signature-based and statistical-based IDS are **easy** to be subverted. For instance, zero-day attacks are not captured by signature-based IDS, whereas statistical-based IDS is prone to data corruption due to the limited number of samples to build its baseline model. Machine-learning based IDS is more difficult (**moderate**) to be subverted but is susceptible to data poisoning attacks during the learning phase. Physics-based IDS is **hard** to be subverted since the attacker needs to ensure the physical constraints of the system is fulfilled. In general, anomaly-based IDSes suffer from a high false positive/negative rate. Thus, anomaly-based IDSes are **partial**ly mature whereas signature-based IDSes are **fully** mature.

### D. Remote Attestation

Software or firmware on embedded devices can be compromised by attackers through remote malware injection or physical attacks on the network [8], [30]. Two general methods have

TABLE III
RESULTS OF COMPARATIVE STUDY OF DEFENSE MECHANISMS

| Defense mechanism | | Cost | | | Intrusiveness | Protection Coverage | | Exploitability | Maturity |
|---|---|---|---|---|---|---|---|---|---|
| | | Deployment | Operating | Maint. | | Asset Type | Attack Phase | | |
| Zoning | Physical | Low | Low | Low | Low | PD | AoO | Moderate | Fully |
| | Network | Low | Low | Low | Low | NA | R,D | Easy | Fully |
| IDS | Signature-based | Low | Medium | Medium | Low | ND | R,D,E,I,C&C,AoO | Easy | Fully |
| | Statistical-based | Low | Low | Low | Low | ND | R,D,E,I,C&C,AoO | Easy | Partial |
| | Machine-learning | Medium | Low | Medium | Low | ND | R,D,E,I,C&C,AoO | Moderate | Partial |
| | Physics-based | High | Low | High | Low | ND,HD | R,D,E,I,C&C,AoO | Hard | Partial |
| Attestation | Hardware-based | High | Low | High | High | HD | E,I | Hard | Partial |
| | Software-based | Medium | Low | Medium | Medium | HD | E,I | Moderate | Partial |
| Deception | Honeypot | Medium | High | High | Low | NA | R,C&C | Hard | Immature |
| | In-network deception | Medium | Medium | Medium | Medium | NA | R,C&C | Hard | Immature |
| Incident Response | | High | High | Medium | Low | ALL | AoO | Moderate | Fully |
| Secure Policies and Protocols | | High | High | High | High | ND,HD | R,D | Hard | Partial |

PD=Physical Device; NA=Network Access; HD=Host Data; ND=Network Data

R=Reconnaissance; W=Weaponization; D=Delivery; E=Exploitation; I=Installation; C&C=Command and Control; AoO=Actions on Objective

been proposed to provide software attestation: (1) software-based and (2) hardware-based. In software-based attestation, a prover must prove to the verifier that the checksum computed based on the content of its Random Access Memory (RAM) footprint, including its current operating status (e.g. program counter value) is correct [31]. Hardware-based attestation uses a Trusted Platform Module (TPM) [32] which runs a challenge-response protocol based on a public key encryption scheme to verify the integrity of the software.

*Discussion:* Remote attestation has a **low** operating cost. Hardware-based attestation has **high** deployment and maintenance cost as compared to software-based attestation which has **medium** cost. That is because every device requires a TPM to conduct hardware-based attestation which is costly due to the huge number of legacy devices in SG. Hardware-based attestation is also **high**ly intrusive as compared to software-based attestation which is only mildly (**medium**) intrusive. One reason is that hardware-based attestation requires the installation of a TPM, which puts trust on the person who designed it, while software-based attestation requires only minor software upgrades. Remote attestation protects the **host data** from the **exploitation and installation** attack phase and is **partial**ly mature due to cost constraints (hardware-based) and latency constraints (software-based). In terms of exploitability, software-based attestation is **moderate** given that some of the vulnerabilities such as strict timing guarantees and proxy attacks (i.e., the device under attestation can ask a more powerful remote device to compute the checksum) have been overcome by recent advances in technology. Hardware-based attestation is **hard** to be subverted because the TPM self-destructs when it detects tampering. However, this approach cannot detect memory modifications during runtime.

### *E. Deception Technology*

Deception technologies aim at fooling and confusing attackers by means of well-crafted "decoy" systems or devices. A typical deception mechanism is a honeypot. The honeypot presents itself as a valuable, vulnerable target to the attacker, misleads the attacker in a sandbox environment to slow down attacks and collect threat intelligence. In the SG, the capabilities of the honeypot have been extended beyond emulating network topology and services to emulate the dynamic physical properties of the system (e.g., the device states of circuit breakers [33], [34] including a honeypot network called a honeynet [35]). While honeypots are usually isolated from the real system, another approach involves the deployment of virtual, decoy devices inside the production network, which we call in-network deception. For example, [36] utilizes software-defined network (SDN) to dynamically change the connectivity of field devices (i.e., shuffling online/offline devices) over time and utilize offline devices as decoys to confuse attackers.

*Discussion:* Deception technologies are virtual, software-based implementation, so their deployment cost is **medium**. In terms of operating and maintenance costs, honeypot systems have **high** costs compared to in-network deception approach which has **medium** costs because the honeypot requires continuous monitoring to handle alarms and analyze collected logs. On the other hand, in-network deception requires operators' attention only when suspicious activities are detected, so intensive monitoring is usually not required after deployment. Honeypots have **low** intrusiveness because they are isolated from the production system. By contrast, in-network deception approaches are more intrusive (**medium**) because the virtual devices run on the substation gateway or IDS appliances. Deception technologies protect **network access** by quarantining the attacker in the **reconnaissance** and **command and control** attack phase and are **hard** to subvert because the attacker is unaware of the real system services and operation. However, deception technology is an **immature** mechanism.

### *F. Incident Response*

Once attacks are detected, it is important to implement an incident response plan that guides the organization to respond and recover quickly, so that damage caused by the

security incidents can be mitigated [17]. Several studies have investigated how the response process can be automated using SDN, Network Function Virtualization (NFV) [37], and game theory [38]. This will greatly improve the response time, allowing the Computer Security Incident Response (CSIR) team to concentrate on more important tasks. Other works on automating incident response include classifying incidents to better assist the CSIR team to quickly forward the requests to the appropriate team for corrective actions [39].

*Discussion:* Despite many efforts to automate the response process, incident response still exhibits **high** deployment and operating costs, but **medium** maintenance cost due to the need to hire experienced personnel and the need to retrain them on a regular basis. Incident response is **low**ly intrusive to the system because it only acts when a security breach has occurred. For the same reason, it can only protect against **actions on objective** attack phase. In terms of protection coverage, incident response protects **all** assets against future attacks through patch management and policies. It is **hard** to subvert because it is a **fully** mature technology that has been implemented for a long time. Most issues have already been rectified.

### G. Defense Compatibility

In this study, we designed a $6 \times 6$ matrix in Table IV to determine the compatibility of a defense mechanism. As shown in Table IV, zoning mechanisms have no major dependency that may conflict with other mechanisms being deployed. IDS is usually deployed together with firewalls, so it depends on network zoning mechanisms. IDS also depends on deception technologies as the two need to interact to reduce the number of potential false detections that may occur as a result of their deployment. However, IDS is in conflict with secure protocols, especially when the traffic is encrypted. Remote attestation, in general, has two dependencies. First, software-based attestation depends on zoning mechanisms such as firewalls to prevent proxy attacks. Second, it is dependent on secure protocols like cryptography for security. Deception technologies depend on network zoning (if it is deployed on the internal network) for greater security and secure protocols to emulate services. Finally, incident response depends on remote attestation, deception technology, and IDSes for malicious reports to initiate recovery plans but may conflict with the standard use of secure protocols. For example, the CSIR team may use Telnet instead of SSH for remote configurations.

TABLE IV
PAIRWISE COMPARISONS OF THE COMPATIBILITY BETWEEN DEFENSE MECHANISMS; EITHER (1) (D)EPENDENT ON, (2) (N)EUTRAL, OR (3) (C)ONFLICTING WITH ANOTHER MECHANISM.

| Defense Mechanism | (1) | (2) | (3) | (4) | (5) | (6) |
|---|---|---|---|---|---|---|
| Zoning (1) | | N | N | N | N | N |
| IDS (2) | D | | N | D | N | C |
| Remote Attestation (3) | D | N | | N | N | D |
| Deception Technology (4) | D | N | N | | N | D |
| Incident Response (5) | N | D | D | D | | C |
| Secure policies and protocols (6) | N | C | N | N | C | |

D=Dependency; N=Neutral; C=Conflict

## V. CASE STUDY

In this section, we use our framework to analyze the security of substations and propose a plan for the deployment of several defense mechanisms that we discussed earlier. First, we verify the rationale of existing security deployments in substations using our framework. Substations need to comply with NERC CIP (North American Electric Reliability Corporation critical infrastructure protection) regulations which require enforcement of cyber and physical security. Thus, substations have deployed physical and network zoning, incident response teams, secure policies and protocols, and signature-based IDSes [40]. From Table III, we note that most of those defense mechanisms deployed by the substations have low intrusiveness and focus primarily on protecting network access and data.

However, as the Ukraine incident has shown, it is inadequate to focus security solutions on protecting network data alone. We suggest a short-term and long-term deployment strategy for substations using our framework. A short-term solution would be to extend the protection coverage of the system to host data and physical devices in the system using defense mechanisms that have low cost and intrusiveness. We suggest deploying remote attestation to protect against malicious CrashOverride Malware [3] as was performed in the Ukraine incident. As a long-term solution, defense mechanisms that are harder to exploit can be deployed to protect the system against more sophisticated attacks such as those in the Ukraine incident. We suggest the deployment of more complex IDSes such as physics-based IDSes, and deception technologies. Although those defense mechanisms' cost is high, they provide additional layers of defense. For example, physics-based IDSes monitor the physical processes and would be alerted by the attacker's action of opening circuit breakers in the Ukraine incident. Deception technologies are also an emerging solution to delay the attacker while learning about the attacker's intentions. Thus, our framework allows us to analyze the security posture of a substation and suggest defense mechanisms based on our study of existing high-profile attacks.

## VI. CONCLUSION

In this paper, we provide a comprehensive review of the defense mechanisms in SG from a defense-in-depth perspective. We proposed a pragmatic framework for comparing the various defense mechanisms. Comparative and compatibility analyses were performed using the metrics defined by our framework to determine their strengths, weaknesses, and interdependencies. Using the Ukraine incident as a case study, we conclude that there is no "one-size-fits-all" solution. The best strategy is to adopt the defense-in-depth approach by employing many layers of defense to include the security of host data and software on physical devices. In this regard, remote attestation and honeypots are two viable options worth considering.

## ACKNOWLEDGMENT

This research is supported in part by the National Research Foundation, Prime Minister's Office, Singapore under the Energy Programme and administrated by the Energy Market Authority (EP Award No.NRF2017EWT-EP003-047), and in part by the National Research Foundation, Prime Minister's Office, Singapore under its Campus for Research Excellence and Technological Enterprise (CREATE) programme.

## REFERENCES

[1] G. Kunz, J. Machado, E. Perondi, and V. Vyatkin, "A formal methodology for accomplishing IEC 61850 real-time communication requirements," *IEEE Trans. Ind. Electron.*, vol. 64, no. 8, pp. 6582–6590, 2017.

[2] H. Yoo and T. Shon, "Challenges and research directions for heterogeneous cyber-physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture," *Futur. Gener. Comput. Syst*, vol. 61, pp. 128–136, 2016.

[3] I. Dragos, "Crashoverride: Analysis of the threat to electric grid operations." [Online]. Available: https://dragos.com/wp-content/uploads/CrashOverride-01.pdf

[4] M. Strobel, N. Wiedermann, and C. Eckert, "Novel weaknesses in IEC 62351 protected smart grid control systems," in *IEEE Int. Conf. on SmartGridComm*, Nov 2016, pp. 266–270.

[5] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in *IEEE Globecom Workshops*, Dec 2012, pp. 1508–1513.

[6] N. Kush, E. Ahmed, M. Branagan, and E. Foo, "Poisoned GOOSE: Exploiting the GOOSE protocol," in *Proc. 12th Australasian Inform. Security Conf.*, 2014, pp. 17–22.

[7] B. Moussa, M. Debbabi, and C. Assi, "A detection and mitigation model for PTP delay attack in an IEC 61850 substation," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 3954–3965, 2018.

[8] N. Govil, A. Agrawal, and N. O. Tippenhauer, "On ladder logic bombs in industrial control systems," in *Comput. Security*. Springer, 2017, pp. 110–126.

[9] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, 2004.

[10] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Comput. Surveys*, vol. 48, no. 3, p. 37, 2016.

[11] C. Iheagwara, A. Blyth, and M. Singhal, "Cost effective management frameworks for intrusion detection systems," *J. Comput. Security*, vol. 12, no. 5, pp. 777–798, 2004.

[12] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surveys*, vol. 46, no. 4, pp. 1–29, March 2014.

[13] G. Elbez, H. B. Keller, and V. Hagenmeyer, "A New Classification of Attacks against the Cyber-Physical Security of Smart Grids," in *Proc. 13th Int. Conf. Availability, Rel. and Security*. ACM, 2018, p. 63.

[14] L. Martin, "The Cyber Kill Chain®." [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[15] A. Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, "Toward Threat of Implementation Attacks on Substation Security: Case Study on Fault Detection and Isolation," *IEEE Trans. Ind. Electron.*, vol. 14, no. 6, pp. 2442–2451, 2018.

[16] P. T. Manditereza and R. C. Bansal, "Introducing A New Type of Protection Zone for the Smart Grid Incorporating Distributed Generation," in *IEEE ISGT Asia*. IEEE, 2018, pp. 86–90.

[17] D. Kuipers and M. Fabro, *Control systems cyber security: Defense in depth strategies*. United States. Department of Energy, 2006.

[18] "IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems," pp. 1–38, 2015.

[19] S. Manson and D. Anderson, "Practical cybersecurity for protection and control system communications networks," in *Petroleum and Chemical Ind. Tech. Conf. (PCIC), 2017*. IEEE, 2017, pp. 195–204.

[20] R. Schlegel, S. Obermeier, and J. Schneider, "Assessing the security of IEC 62351," in *Proc. 3rd Int. Symp. for ICS & SCADA Cyber Security Res.*, 2015, pp. 11–19.

[21] R. Udd, M. Asplund, S. Nadjm-Tehrani, M. Kazemtabrizi, and M. Ekstedt, "Exploiting bro for intrusion detection in a SCADA system," in *Proc. 2nd ACM Int. Workshop on CPSS*. ACM, 2016, pp. 44–51.

[22] J. Zhang, S. Gan, X. Liu, and P. Zhu, "Intrusion detection in SCADA systems by traffic periodicity and telemetry analysis," in *Comput. and Commun. (ISCC), 2016 IEEE Symp. on*. IEEE, 2016, pp. 318–325.

[23] W. Ren, T. Yardley, and K. Nahrstedt, "EDMAND: Edge-Based Multi-Level Anomaly Detection for SCADA Networks," in *IEEE Int. Conf. SmartGridComm*. IEEE, 2018, pp. 1–7.

[24] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," *ACM Comput. Surveys*, vol. 51, no. 4, pp. 1–36, July 2018.

[25] D. I. Urbina, J. A. Giraldo, A. A. Cardenas, N. O. Tippenhauer, J. Valente, M. Faisal, J. Ruths, R. Candell, and H. Sandberg, "Limiting the impact of stealthy attacks on industrial control systems," in *Proc. 2016 ACM SIGSAC Conf. CCS*. ACM, 2016, pp. 1092–1105.

[26] D. Mashima, B. Chen, T. Zhou, R. Rajendran, and B. Sikdar, "Securing substations through command authentication using on-the-fly simulation of power system dynamics," in *IEEE Int. Conf. SmartGridComm 2018*. IEEE, 2018, pp. 1–7.

[27] D. Mashima, P. Gunathilaka, and B. Chen, "Artificial command delaying for secure substation remote control: Design and implementation," *IEEE Trans. Smart Grid*, 2017.

[28] H. Lahza, K. Radke, and E. Foo, "Applying domain-specific knowledge to construct features for detecting distributed denial-of-service attacks on the GOOSE and MMS protocols," *Int. J. of Crit. Infr. Prot.*, vol. 20, pp. 48–67, 2018.

[29] P. Schneider and K. Böttinger, "High-Performance Unsupervised Anomaly Detection for Cyber-Physical System Networks," in *Proc. Workshop CPS-SPC*. ACM, 2018, pp. 1–12.

[30] L. Garcia, F. Brasser, M. H. Cintuglu, A.-R. Sadeghi, O. A. Mohammed, and S. A. Zonouz, "Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit." in *NDSS*, 2017.

[31] B. Chen, X. Dong, G. Bai, S. Jauhar, and Y. Cheng, "Secure and efficient software-based attestation for industrial control devices with arm processors," in *Proc. 33rd Annu. Comput. Security Appl. Conf.* ACM, 2017, pp. 425–436.

[32] N. Asokan, F. Brasser, A. Ibrahim, A.-R. Sadeghi, M. Schunter, G. Tsudik, and C. Wachsmann, "Seda: Scalable embedded device attestation," in *Proc. 22nd ACM SIGSAC Conf. Comput. and Commun. Security*. ACM, 2015, pp. 964–975.

[33] K. Koltys and R. Gajewski, "SHaPe: A honeypot for electric power substation," pp. 37–43, 01 2015.

[34] D. Antonioli, A. Agrawal, and N. O. Tippenhauer, "Towards high-interaction virtual ics honeypots-in-a-box," in *Proc. 2nd ACM Workshop Cyber-Physical Syst. Security and Privacy*. ACM, 2016, pp. 13–22.

[35] D. Mashima, B. Chen, P. Gunathilaka, and E. L. Tjiong, "Towards a grid-wide, high-fidelity electrical substation honeynet," in *IEEE Int. Conf. SmartGridCommun*, Oct 2017, pp. 89–95.

[36] H. Lin, Z. Kalbarczyk, and R. K. Iyer, "Raincoat: Randomization of network communication in power grid cyber infrastructure to mislead attackers," *IEEE Trans. SmartGrid*, pp. 1–14, 2018.

[37] A. F. M. Piedrahita, V. Gaur, J. Giraldo, A. A. Cardenas, and S. J. Rueda, "Leveraging software-defined networking for incident response in industrial control systems," *IEEE Softw.*, vol. 35, no. 1, pp. 44–50, 2018.

[38] S. A. Zonouz, H. Khurana, W. H. Sanders, and T. M. Yardley, "RRE: A game-theoretic intrusion response and recovery engine," *IEEE Trans. Parallel Distrib. Syst*, vol. 25, no. 2, pp. 395–406, 2014.

[39] R. de Jesus Martins, L. A. D. Knob, E. G. da Silva, J. A. Wickboldt, A. Schaeffer-Filho, and L. Z. Granville, "Specialized CSIRT for Incident Response Management in Smart Grids," *J. Netw. Syst. Manag.*, vol. 27, no. 1, pp. 269–285, 2019.

[40] J. Hallenstein, "Review of cyber and physical security protection of utility substations and control centers." [Online]. Available: http://www.psc.state.fl.us/Files/PDF/Publications/Reports/General/Electricgas/Cyber_Physical_Security.pdf