Attack Tree Analysis of a Digital Secondary System in an Electrical Substation

Mauricio Silveira, David Dolezilek, Scott Wenke, and Jaya Yellajosula
Schweitzer Engineering Laboratories, Inc.

Presented at the
16th International Conference on Developments in Power System Protection
Hybrid Format (virtual and in-person at Newcastle Gateshead, United Kingdom)
Presented Virtually
March 7–10, 2022

ATTACK TREE ANALYSIS OF A DIGITAL SECONDARY SYSTEM IN AN ELECTRICAL SUBSTATION

Mauricio Silveira[1], David Dolezilek[1], Scott Wenke[1], Jaya Yellajosula[1]*

[1]Schweitzer Engineering Laboratories, Inc., Pullman, Washington, USA
**Mauricio_Silveira@selinc.com*

Keywords: CYBERSECURITY, PROCESS BUS, DIGITAL SECONDARY SYSTEM, PRIVACY, SECRECY.

Abstract

Modern digital secondary system (DSS) technology uses digital communications among relays and remote digital sensors over high-speed fiber connections to perform fault detection and trip circuit control. A cyber vulnerability assessment of each proposed communications design is essential to evaluate the energy control system's reliability. Many cybersecurity technologies from numerous industries are promoted for use in DSS communications with unknown impacts. This paper introduces appropriate metrics and a cyber vulnerability assessment framework, using the attack tree method, to compare the cyber risk of available technologies to determine the dependability and security of digital control and protective trip circuits.

1 Introduction

This paper is a subset of [1] and introduces the attack tree analysis (ATA), an event tree method to quantify the risk of a successful attack to a system by combining all cyber vulnerabilities as branches. ATA is a tool to quantify metrics of vulnerabilities to compare, avoid, and mitigate them. Cyber vulnerabilities are easy to name, but their relative cyberthreats, or the probability of their success, was previously difficult to quantify. Methods introduced in this paper use ATA to analyze the probability of success for each threat so that they can be identified as individual branches in a system's ATA. The result of an ATA quantifies the top event as the threat availability of the attack. Other threat modeling tools are available, such as the MITRE ATT&CK framework knowledge database [2]. ATA can be combined with the MITRE ATT&CK to create robust metrics for more generic cybersecurity issues.

It is common to design for hardware availability by evaluating the reliability and maintainability based on mean time to diagnose (MTTD) failure and mean time between failure (MTBF) information. MTBF provides a comparison of the unavailability to serve the intended purpose among different component choices. Previously, the comparison of cyberthreats was not possible due to the lack of a universal comparison metric. The metric introduced in this paper, threat availability, is used to measure and contrast the potential success of a cyberattack or mitigation control. The Common Vulnerability Score System (CVSS), as documented by the National Institute of Standards and Technology (NIST), is a publicly available tool for the assessment and comparison of information technology (IT) vulnerabilities and is often used to drive correct actions for commercial and corporate networks. The CVSS scoring tool is used in this paper to understand and contrast operational technology (OT) vulnerabilities; however, because of the difference in their purpose, scores for OT methods created by this tool should not be directly compared with scores created for IT methods using this tool. There is an effort by the cyber community to consider modifying the CVSS score system for OT environments [3]. In the absence of that modification, this paper uses the CVSS score system, combined with other operational impact metrics, to create a tailored OT cyber vulnerability assessment.

The focus of this paper is to improve the design process for the energy control system to detect, respond to, and survive a threat specifically by introducing the threat availability metric to understand the probability of a successful attack associated with each cyber vulnerability.

2 Cyber Vulnerability Assessment Applied to Digital Secondary Systems (DSSs) Using an Attack Tree

An ATA is a graphical visualization method capable of measuring cyberthreats of a cybernetic system [4]. The attack tree consists of hierarchical nodes that aim to measure theoretical security breaches against proposed countermeasures, that provide a baseline comparison between different solutions, and that are used to understand threats as they evolve.

The attack tree modeling is a simple and visual method of organizing cyber intelligence information, allowing system architecture engineers to make security decisions during the project's specification phase without the need for complex threat modeling or simulations.

This paper's proposed ATA is tailored toward the process bus within the DSS application and is shown in Fig. 1. At the top of the tree are three root nodes, confidentiality, integrity, and availability (CIA), representing the attack's malicious goal or other unintended consequences. In a DSS system context, the CIA index means the following:

- Confidentiality: the system's ability to keep data sharing contained to only trusted peers' devices.
- Integrity: the system's level of confidence and trust in shared data.
- Availability: the system's capability to ensure data are shared during and after failure events.

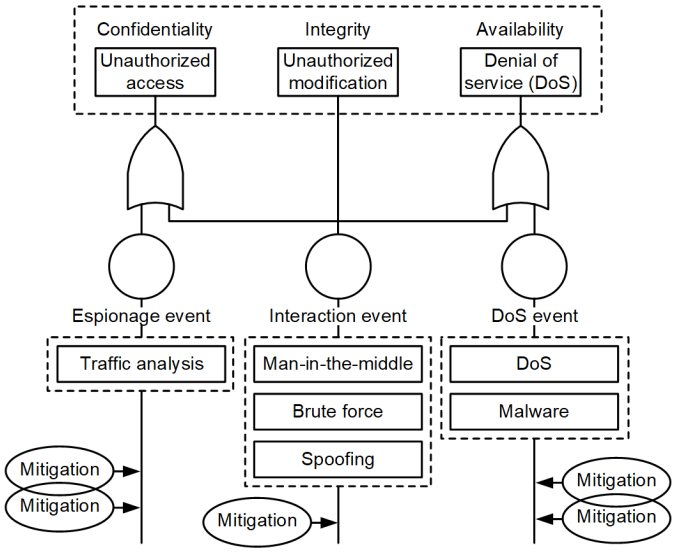

Fig. 1. Attack tree applied to DSS.

In sequence, the root nodes are decomposed into several subtasks representing cyberattack threat events, and mitigation leaves characterize countermeasures.

2.1 Espionage Events

Espionage events are situations when the attacker gains access to observe and analyze data not intended for them. Analysis of illegitimately collected communications traffic may be harmful when confidential information, such as keys and passwords, are observed as they pass an internal system-communication channel without cryptographic protection.

The use of plaintext credentials in a protected substation local-area network (LAN), such as to a process bus device, is a valuable capability because it provides uninterrupted, uncomplicated, and interoperable engineering access authorization. The value of this capability is favorably balanced against the likelihood of exploitation from an espionage event bypassing LAN perimeter protection. Cryptographic protection of this traffic if it leaves the LAN, such as to a wide-area network (WAN), may use secrecy to hinder espionage outside the LAN perimeter.

2.2 Interaction Events

Interaction events represent the attacker's ability to manipulate the system actively and compromise its operation, either through the network (data manipulation and communications suppression) or physically (cutting communication cables). Data manipulation attack vectors exist as unintended consequences of process bus test methods which use false, or simulated, signals. Interaction events are considered a common degradation entity to all the root nodes' indexes.

2.3 DoS Events

The goal of denial of service (DoS) events is to exhaust resources and prevent needed communication from happening. Usually, during a DoS event, the malicious entity has access to the local network and can freely send packets (from malware installed in the local computer workstation). Note that these packets do not need to be considered valid; they only need to exhaust network resources, thereby preventing legitimate communications from happening [5].

2.4 Mitigation Leaves

In ATA, mitigation techniques to minimize the cybersecurity risk are represented by mitigation leaves. In this section, the proposed mitigation techniques are discussed based on a DSS application. While many mitigation techniques could be deployed to secure a DSS, for the sake of brevity this paper focuses on the following measures, which are commonly used for these systems:

- Cryptography via encryption and authentication
- Network architecture

2.4.1 Cryptography

Fig. 2 represents the encryption and decryption process. Encryption uses a mathematical function *e()* to create data confusion and diffusion based on the sequence input data *x[n]* and a shared key *k*. The encryption function can be reversed using the decryption function *d()* and the same shared key *k* pair. Encryption can hide information from a malicious source viewing the nonsecure channel, but it cannot validate the source of information.

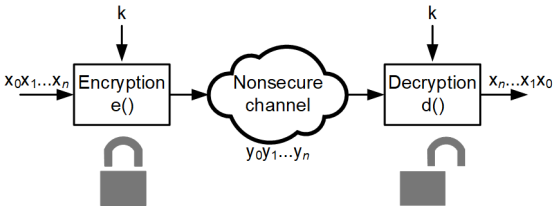

Fig. 2. Encryption and decryption functions.

Encryption and authentication may be good options for use on non-real-time networks that need to be flexible and accommodate a dynamic number of devices. However, they add significant latency, due to the computational cost of encrypting and decrypting data, and complexity, because of the key rotation mechanism process needed to maintain the cryptosystem safe. In DSS applications, because the traffic is related to power system protection, it is real-time-sensitive, such as IEC 61850 Sampled Values (SV) signals. Therefore, encryption solutions can be a drawback to the SV system's performance, even unacceptably so. While it is recognized that encryption delays may have a negative impact at the typical SV sampling and publication rates, future sample rates

will be higher—they always are. Some relays are sampling at a megahertz. Therefore, an encryption solution will most definitely limit future advancements in improving measurement resolution and fidelity.

2.4.2 Network Architecture

In a DSS system, encryption can lead to complex maintenance and add additional latency for real-time applications; however, DSS networks are usually static and rarely change the active topology, which makes them suitable candidates for solutions based on network architectures and traffic segregation. Both solutions' effectiveness comes from the ability to lock the data path channels, allowing only authorized traffic through the communication channels.

The software traffic segregation logically isolates traffic in a multicast network, which can be achieved with technologies like IEEE 802.1Q virtual local-area networks (VLANs) and software defined networking (SDN) for OT applications (OT SDN) [6]. The VLAN implementation segregates traffic by looking at the VLAN tag information in the Ethernet packet. However, VLANs have known vulnerabilities that can be exploited, such as VLAN-hooping [7]. In an OT SDN, as shown in Fig. 3, deny-by-default architecture separates the control and data planes and uses preprogramming flow rules to configure the data paths through the OT SDN network. This approach drastically reduces the vulnerabilities in an Ethernet network since OT SDN does not use media access control tables and locks the communication channels based on the flow controller instructions to prevent any malicious actor from interacting with the network.

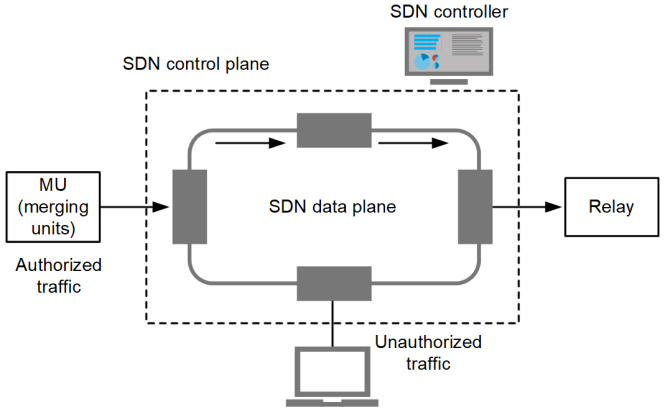

Fig. 3. OT SDN.

Therefore, the choice of network architecture plays a role in the cybersecurity of a DSS. There are several topology references and examples available in the literature, and the IEC TR 61850-90-4 and projects described in [8], [9], and [10] have a variety of network designs applied to the process bus, such as point-to-point, duplicated star, single ring, etc.

However, DSSs have a unique challenge due to the real-time nature and volume of traffic. In many cases, the DSS traffic, from a publisher perspective, is one-way and typically needs to be delivered to two or three devices. Therefore, topologies like point-to-point and point-to-multipoint, as shown in Fig. 4, are attractive from a DSS standpoint because they use physical connections to manage traffic and data exchange. This method can be practically deployed and may provide benefits such as reducing maintenance cost, using a physical device's intrinsic cybersecurity, and increasing reliability due to using fewer devices.

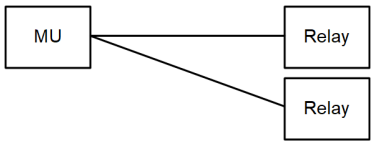

Fig. 4. Point-to-multipoint DSS architecture.

3 Cybersecurity Metrics Applied to DSSs

According to the U.S. Department of Energy, metrics for use in the power grid architecture must be derived from proper system characteristic traits [11]. That means that the cybersecurity metrics related to the power grid, such as DSS, need to include the peculiarities of a real-time sampling acquisition system applied to the control of primary electric power equipment in a substation. Therefore, this section applies cybersecurity metrics from a DSS perspective.

3.1 Threat Availability (TA)

The threat availability (TA) leaf index is a combined metric based on the vulnerability score and the power outage operational metrics related to the consequences of a successful attack. The index TA is calculated according to (1).

$$TA = \sum_{i-1}^{n} VS + \sum_{i-1}^{n} PowerOutageConsequences \quad (1)$$

The first part of the equation is the vulnerability score (VS), which represents the severity of the exploited vulnerability. As a novel and useful method, the authors use the CVSS score system traditionally used for IT applications and adapt it for use in analysis of OT systems. The CVSS is an open-framework metric tool managed by NIST and used as a standard score to measure cybersystems' vulnerabilities. As mentioned, the scores used for this paper are intended for the specific use of contrasting threats to DSS communications and not for comparison with commercial applications or scores.

In this paper, the authors consider the base CVSS score vector, as described in [1]. The explanation of each score field is out of the scope of this paper and can be found in [1] and [12].

The second component of (1) is the operational electrical substation relative disruption metric, which is a unitless value equal to the quantity of power outage hours resulting from a successful cyberattack. Reference [1] details the vulnerability considerations used in this paper. Therefore, the index TA is a unitless measure of the threat availability, or severity of the system's vulnerability, tailored to a cyber event in an electric substation environment.

3.2 Cyber Mitigation of Leaf (Ω)

The cyber mitigation index Ω is a unitless metric that measures the system's resilience to cyberattacks due to a specific mitigation method, and is scored according to (2):

$$\Omega = Resilience - Complexity \quad (2)$$

Each of the equation installments has a low, medium, or high weight value, as shown in Table 1. The weight levels can vary according to the user's experience and comfort level with the mitigation solution. Therefore, this section will support the Ω levels chosen for this study case.

Table 1 Cyber mitigation weights

Level	Value
Low	0–3
Medium	4–6
High	7–10

For the Ω levels in this case study, a system resilience of 0 represents the most vulnerable system, and a resilience of 10 is the least vulnerable system. According to the Presidential Policy Directive/PPD-21, resilience for the power grid is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions" [13].

In this paper, resilience will be measured according to the historical hardness of the mitigation method. For example, the National Security Agency (NSA) released a recommendation note that exposed the encryption's history hardness for Transport Layer Security (TLS) cipher suites; Table 2 shows the cipher suite's situation awareness [14].

Table 2 Encryption cipher suite situation

Cipher suite	Situation
RC2	Obsolete
RC4	Obsolete
DES	Obsolete
IDEA	Obsolete
3DES	Obsolete
AES	Active

Complexity is the measurement of implementation cost and system maintenance; complexity can also be correlated with the costs and benefits of a solution [15]. For example, state-of-the-art encryption has an excellent resilience against cyberattacks. However, its maintenance cost is still high due to the key exchange maintenance and the need to update the encryption in the field after it becomes computationally obsolete. However, if the device has the capability of third-factor authorization of the read/write (R/W) access control, then it can act as the low-complexity authentication process, providing a high level of resilience against interaction events. Reference [1] summarizes the resilience and complexity levels chosen for this experiment and the applicable buses.

3.3 CIA Root

Equations (3), (4), and (5) are derived by the attack tree shown in Fig. 1.

$$\mathrm{C_{Root}} = \left(\mathrm{TA_{Espionage}} - \Omega_{\mathrm{Confidentiality}}\right) + \left(\mathrm{TA_{Interaction}} - \Omega_{\mathrm{Integrity}}\right) \quad (3)$$

$$\mathrm{I_{Root}} = \left(\mathrm{TA_{Interaction}} - \Omega_{\mathrm{In\,tegrity}}\right) \quad (4)$$

$$\mathrm{A_{Root}} = \left(\mathrm{TA_{DoS}} - \Omega_{\mathrm{Availability}}\right) + \left(\mathrm{TA_{Integrity}} - \Omega_{\mathrm{Availability}}\right) \quad (5)$$

The CIA root indexes are the metrics used to compare the cybersecurity risk among different DSS topologies. Note that the CIA root indexes are a comparative metric and should be used to compare similar systems and solutions.

4 DSS Cybersecurity Vulnerability Assessment Evaluation

This section evaluates one scenario with a total of three cases to illustrate the use of threat availability analysis to compare and contrast design choices. The scenario considers a common network-switched station bus with encryption and three different process bus DSS architectures:

- Case 1: point-to-point process bus
- Case 2: multicast network-switched process bus
- Case 3: OT SDN process bus

In all three case study architectures, the relays are connected to the station bus for engineering access and supervisory control and data acquisition (SCADA) purposes. Therefore, all the vulnerabilities related to the station bus are common across the proposed solutions. The goal is to define a cyber VS for three process bus variant solutions.

4.1 Station Bus TA Leaves

Table 3 represents the TA values for each of the station bus communication types. As a comparison metric, these values are not inherently bad or good except with respect to one another. The individual TA indexes are computed related to potential cyberthreat events corresponding to each communication type allowed on the station bus, and the overall CIA VS of the station bus is the sum of each of the TA results.

Table 3 Cyberattack leaves results for station bus communications bus

Communication type	$TA_{\mathrm{Espionage}}$	$TA_{\mathrm{Interaction}}$	TA_{DoS}
Sniffing station bus	7.5	—	—
SCADA	—	13.4	—
Brute-force attack	—	6.3	—
Station bus malware	—	0	7.5
Read-only engineering access	—	5.1	—
R/W engineering access	—	12.2	—
TA_{Total}	7.5	37	7.5

4.2 Total Cyberattack Leaves

Table 4, Table 5, and Table 6 represent the process bus TA leaves values from Cases 1–3. Each table has the respective VS for the station and process buses. The individual TA indexes are computed for each corresponding cyberattack event, and the overall VS of the solution is the sum of the station and process bus TA results.

Table 4 Case 1: TA leaves results for Case 1

Case 1	$TA_{Espionage}$	$TA_{Interaction}$	TA_{DoS}
Station bus	7.5	37	7.5
Process bus	3.8	6.8	3.9
TA_{Total}	11.3	43.8	11.4

Table 5 Case 2: TA leaves results for Case 2

Case 2	$TA_{Espionage}$	$TA_{Interaction}$	TA_{DoS}
Station bus	7.5	37	7.5
Process bus	6.2	7.5	5
TA_{Total}	13.7	44.5	12.5

Table 6 Case 3: TA leaves results for Case 3

Case 3	$TA_{Espionage}$	$TA_{Interaction}$	TA_{DoS}
Station bus	7.5	37	7.5
Process bus	3.8	6.8	3.9
TA_{Total}	11.3	43.8	11.4

4.3 Cyber Mitigation Leaves

This section evaluates the impact of potential mitigation techniques for Cases 1–3. The station bus mitigation techniques picked for this experiment are the encryption and authentication of data. Table 7, Table 8, and Table 9 show the process bus mitigation leaf values from Cases 1–3.

Table 7 Case 1: Mitigation leaves values for station bus with cryptography plus point-to-point process bus

Case 1	$\Omega_{Confidentiality}$	$\Omega_{Integrity}$	$\Omega_{Availability}$
Station bus	3	2	1
Process bus	7	7	7
Ω_{Total}	10	9	8

Table 8 Case 2: Mitigation leaves values for station bus with cryptography plus multicast network-switched process bus

Case 2	$\Omega_{Confidentiality}$	$\Omega_{Integrity}$	$\Omega_{Availability}$
Station bus	3	2	1
Process bus (VLANs)	2	2	2
Ω_{Total}	5	4	3

Table 9 Case 3: Mitigation leaves values for station bus with cryptography plus OT SDN process bus

Case 3	$\Omega_{Confidentiality}$	$\Omega_{Integrity}$	$\Omega_{Availability}$
Station bus	3	2	1
Process bus	5	5	5
Ω_{Total}	8	7	6

4.4 CIA Indexes Results

Fig. 5 shows the results from the CIA VS according to (3), (4), and (5) as applied to each of the three process bus topologies.

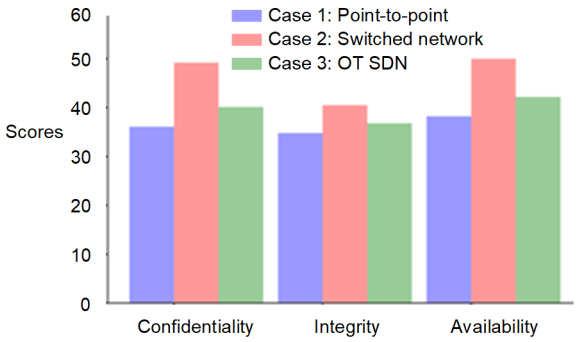

Fig. 5. CIA vulnerability scores for Cases 1–3 using station bus traditional networking and cryptography.

The results represent the risk of failing to keep data confidential, to maintain functional integrity of the protection system, and to maintain long-term availability of the protection system for the three DSS solutions. The results show that the highest scores, representing the highest threat availability, are always reached by Case 2. Table 10 displays the improvement, over Case 2, of the relative cybersecurity threat availability scores for DSS Case 1 and Case 3. Table 10 shows that point-to-point is more confidential and secure but is less available due to the single point of failure. Of course, this vulnerability is easily mitigated by using two point-to-point connections for each signal.

Therefore, from a cybersecurity perspective, it is reasonably secure to exchange signals from the yard to the control house using a dedicated architecture such as point-to-point. But when data signal exchange must pass through a network and perhaps be multicast to multiple subscribers, OT SDN is recommended for the process bus switched-Ethernet architecture. Although outside the scope of this paper, the resilience of OT SDN is required to satisfy the performance requirements of process bus SV applications; traditional Ethernet is not appropriate.

Table 10 Relative cybersecurity improvement reduction over Case 2

Process bus architectures	Relative improvement reduction		
	C_{Root}	I_{Root}	A_{Root}
Case 1: Point-to-point	27%	14%	23%
Case 3: OT SDN	18%	9%	16%

5 Conclusion

Event trees are often used to graphically evaluate the likelihood of a system component causing success or failure of a design based on its availability to do so. Threat availability, as introduced in this paper, supports the comparison of the likelihood of success of both cyberthreats and mitigation controls.

DSS technology is used to exchange signals from the substation yard to the control house using digital high-speed communication channels. A DSS aims to reduce costs by replacing traditional copper wiring with fiber-optic cables. However, a DSS introduces a cybersecurity vulnerability that needs to be evaluated to understand power system protection reliability.

The ATA used in this paper was tailored toward the DSS application, and three cyberthreats, espionage, interaction, and DoS, were defined. The cyberattack leaves were calculated using the composed metric of the VS score system and the operational power system outage in case the attack was successful. The mitigation leaves were countermeasure techniques applied to mitigate the vulnerabilities associated with the cyberattack leaves. The main goal was to balance the vulnerabilities against the mitigations and draw a baseline CIA comparison between similar solutions and systems.

In this paper, the tailored DSS attack tree was used to analyze three different DSS solutions: point-to-point, network-switched, and OT SDN. The point-to-point architecture used the practical physical connection approach to safeguard its resilience against cyberthreats. The standard switched network segregated the multicast traffic, using VLANs, to keep CIA high. Through the segregation of the control and data plane, OT SDN achieved a deny-by-default architecture to deal with spurious, unwanted, and uncertified data. This approach drastically reduced the network's attack surface, increasing system reliability and resilience against cyberthreats.

The three solutions evaluated a coupled station bus connected to the process bus DSS. The initial evaluation compared the CIA indexes for the three cases and took into consideration that the station bus was protected using encryption and authentication features. The results showed that the process bus point-to-point architecture is the most secure DSS network among the three, followed by OT SDN.

Although DSS technology is a great advancement toward the digitalization of an electric substation, it is critical to understand and measure the cyber risks involved with its operation. This paper introduced a methodology to help design engineers to understand and explore this weakness before deploying these systems.

6 References

[1] Silveira, M., Dolezilek, D., Wenke, S., et al.: "Cyber Vulnerability Assessment of a Digital Secondary System in an Electrical Substation," proceedings of the 74th Annual Conference for Protective Relay Engineers, virtual format, March 2021.

[2] MITRE ATT&CK: "ATT&CK Matrix for Enterprise," available: attack.mitre.org, accessed January 22, 2021.

[3] Securing ICS: "Industrial Vulnerability Scoring System (IVSS)," available: securingics.com/IVSS/IVSS.html, accessed January 26, 2021.

[4] Ten, C. W., Liu, C. C., Govindarasu, M.: "Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees," proceedings of the IEEE Power Engineering Society General Meeting, Tampa, FL, June 2007.

[5] Silveira, M., Franco, P.: "IEC 61850 Network Cybersecurity: Mitigating GOOSE Message Vulnerabilities," proceedings of the 6th Annual PAC World Americas Conference, Raleigh, NC, August 2019.

[6] Cabral, M., Silveira, M., Urie, R.: "SDN Advantages for Ethernet-Based Control," June 2019. Available: selinc.com.

[7] Hoyos, J., Dehus, M., Brown, T.: "Exploiting the GOOSE Protocol: A Practical Attack on Cyber-Infrastructure," proceedings of the IEEE Globecom Workshops, Anaheim, CA, December 2012.

[8] Dolezilek, D., Dearien, J., Kalra, A.: "Appropriate Testing Reveals New Best-in-Class Topology for Ethernet Networks," proceedings of the 13th International Conference on Developments in Power System Protection, Edinburgh, United Kingdom, March 2016.

[9] Meine, R.: "A Practical Guide to Designing and Deploying OT SDN Networks," proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2019.

[10] IEC 61850-90-4:2020, *Communication networks and system for power utility automation - Part 90-4: Network engineering guidelines*.

[11] Taft, J. D.: "Electric Grid Resilience and Reliability for Grid Architecture," prepared for the U.S. Department of Energy, November 2017. Available: gridarchitecture.pnnl.gov/media/advanced/ Electric_Grid_Resilience_and_Reliability.pdf.

[12] NIST: "National Vulnerability Database." Available: nvd.nist.gov/vuln-metrics/cvss.

[13] The White House: "Presidential Policy Directive -- Critical Infrastructure Security and Resilience," available: obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, accessed January 21, 2021.

[14] NSA: "Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations," January 2021. Available: media.defense.gov/2021/Jan/05/2002560140/ -1/-1/0/ELIMINATING_OBSOLETE_TLS_ UOO197443-20.PDF.

[15] Bewley, J. D., Zhang, R., Charton, T.: "Prioritization and Cost/Benefit Analysis of Cyber Security Controls Within Existing Operational Technology Environments," proceedings of the 15th International Conference on Developments in Power System Protection, virtual format, December 2020.