Cyber Vulnerability Assessment of a Digital Secondary System in an Electrical Substation

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

***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.**

I. Introduction

Event tree analysis (ETA) is a logical method of analyzing the failure or success of a system by modeling each of the system elements that impact the analyzed event (or top event) as the leaves on the event tree. Event trees model the underlying events that impact the success or failure of the top event and calculate the probability of their impact using Boolean logic. The result of the Boolean logic provides a unitless metric that quantifies the analyzed design for comparing the success or failure of various designs that might cause the top event [1].

A digital secondary system (DSS) is a substation control system with communications among both process-level devices and devices at other levels in the station. Station bus communications are connections and protocols that transmit and receive system, engineering, and configuration information and send operator commands to networked intelligent electronic devices (IEDs). Process bus communications are connections and protocols that exchange input/output (I/O) process information between IEDs and process instrumentation and control devices.

The cost and the speed of energy control system (ECS) designs are easily compared as capital plus operations and maintenance (O&M) dollars and operational latency, respectively. These can both be measured; however, system reliability is often compared as the unavailability of each design based on an event tree comparing failure modes, known as fault tree analysis (FTA). FTA compares the failure of each of ECS's designs to perform a top event, such as unavailability to correctly trip a feeder breaker, based on evidence of how frequently components fail while in service as measured by mean time between failure (MTBF). The more unavailable a design is, the greater the risk of failure. The unitless unavailability metric is also used to predict annual downtime and O&M cost based on hardware failure rates [2].

Attack tree analysis (ATA) provides an event tree method to quantify the risk of a successful attack to a system by combining all cyber vulnerabilities as branches. Like FTA, 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 [3]. ATA can be combined with the MITRE ATT&CK to create robust metrics for more generic cybersecurity issues.

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), 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, these OT scores should not be compared with IT scores. There is an effort by the cyber community to consider modifying the CVSS score system for OT environments [4] [5]. 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 ECS 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.

II. Applying Limited Vulnerability Design Processes

The limited vulnerability design (LVD) concept is an iterative design technique that improves system performance by identifying application gaps, evaluating the risk they represent, and then mitigating the risks. For example, in this paper the application gaps are security defects and mitigation control gaps. Once a gap is identified, the risk of the weakness causing unintended success or failure must be quantified. ETA is often used to understand risk based on the probability of each event

tree branch and their combinations. For example, ATA is used to quantify the availability of the success of cyberthreats to perform LVD assessment. The results lead to the appropriate use of technologies and a clear and transparent awareness of each gap, which allows engineers to make an informed decision to either avoid the risk, mitigate the risk, or accept the risk [6]. Specifically, the LVD of communications systems relies on ATA to quantify the threat availability so that analysis and improvement are possible.

LVD is often used to create ECS infrastructure capable of detecting accidental and intentional, cyber and physical, and external and internal human threats. If an attack occurs, the ECS should be designed to isolate any resulting damage and improve the survivability for personnel and equipment affected by an event while maintaining continued use of the utility served by the industrial control system (ICS). It is important to select and customize mitigation controls to balance security with usefulness. For example, tools used for traditional internet-facing IT devices that are too secure and make things difficult to operate encourage users to use workarounds and shortcuts. Also, complicated security measures may inhibit the repair of weaponized mitigation controls and provide unfounded trust in communications after a cyberattack.

Using LVD supports the clear, complete, and candid assessment of gaps, risk, and control of vulnerabilities using steps listed here:

1. Identify gaps during initial design review, understand risk associated with each gap.
2. Choose which gaps to mitigate, and how to mitigate them, based on cost, schedule, and performance.
3. Apply mitigation controls to limit vulnerability and document and explain the remaining gaps identified and accepted in the design review as appropriate.
4. Perform factory acceptance testing and then continuously monitor the in-service system for undetected gaps (previously unknown and new vulnerabilities and threats); monitor the performance of mitigation controls, CVEs, and supplier service bulletins to evaluate new in-service gaps.
5. Return to Step 1.

Certain cyber events have occurred that were enabled by the weaponization of transport layer security (TLS) [7], and the unintended proliferation of malware by SolarWinds [8]. These events illustrate the need to consider a feedback loop, such as in Step 4, to evaluate the negative consequences of mitigation controls. Specific to cyber events, some examples include the weaponization of TLS [7], and the unintended proliferation of malware by SolarWinds [8].

The LVD method leads to improved ECS functionality and performance by preventing or reacting to man-made and natural events. ATA improves the design process for the ECS to detect, respond to, and survive a cyberattack specifically by analyzing all cyber communications threats.

Though the threats exist for all communications, this paper is focused on local and remote access to the devices involved in process bus communications as part of the DSS. To ensure that each communication is resilient to attack, LVD must consider all the legitimate station bus and process bus dataflows related to a substation DSS including:

1. Substation automation and remedial action controls.
2. Self-description of device database contents.
3. Device configuration.
4. Client polling of data from the device.
5. Device server reporting of data.
6. Unsolicited notification of device alarms.
7. Commanded control from local- and remote operators or automation logic.
8. Live and simulated event-driven peer-to-peer, machine-to-machine signal and status multicasting.
9. Live and simulated periodic peer-to-peer, machine-to-machine signal and status multicasting.
10. Time synchronization.
11. File transfer.
12. Engineering access command line interface.

III. Cyber Vulnerability, Exposure, Impact, and Adaptation

Unfortunately, industry terminology often mistakenly conflates exposure and vulnerability, but the two are distinct. Where exposure to attack events is impossible to avoid, each cyber vulnerability is analyzed with respect to its threat availability considering the exposure, impact on the power system, and adaptive capacity of the ECS. In this case, risk associated with the vulnerability, as characterized by its threat availability, refers to the probability that an attack will be successful on a DSS device, and exposure refers to the inventory of elements in an area, the station and process bus, and the context in which a cyberattack may occur such as during infrequent reading and writing (R&W) authorization. The impact may be data disclosure or unwanted trip command to a feeder breaker, and adaptive capacity may be absent from the system or may include a block command to the device that prevents the breaker-open operation from a condition-monitoring device that recognizes that this action would create an unwanted grid state. Adaptive mitigation refers to system components that detect and react to an emerging threat in real time by modifying, or adapting, system behavior to be resilient against the threat. In the previous example, the condition-monitoring device is constantly monitoring the present grid state and has preconfigured knowledge of allowed legitimate changes, so that it can effectively block the others.

If devices are not exposed to a cyberattack, then no threat exists, and if devices are only periodically exposed, then characteristics of that exposure condition the threat availability. For example, if no remote R&W engineering access is performed, then there is no threat of exposure of the authorization credentials even when remote connections are compromised. After commissioning, typically relay settings are modified no more often than every five years [9], if ever, and most likely not via remote communications. However, if authorization credentials for R&W engineering access are used for an hour once every five years to modify relay settings from a remote location, then the credentials are at risk of observation one hour out of every five years. For example, if a substation

router has a vulnerability that allows remote observation, an observer would be able to capture an authentication transaction during the first minute of that hour of remote access, and then an intruder could record the transaction for use in a possible playback attack.

OT software-defined networking (OT-SDN) provides a direct adaptation by restricting the use of authorization credentials to a predetermined and specific point in time [10]. Internal device multifactor authentication, supported by a third party, also provides a direct adaptation by restricting the use of authorization credentials to a specific point in time. For example, OT-SDN and internal relay logic can both allow and restrict communications based on third-party authentication supervision.

Contrary to the presence of the hazard, vulnerability and exposure can be influenced by policy and practice. Examples include a utility's best practice to restrict when and where to permit R&W authentication. Policy changes like these have been the main reason behind decreased attacks, rather than changes to the vulnerability threat availability itself, and vice-versa. DSS applications and communications remain static after commissioning, but the dynamics of the vulnerability and exposure of remote and wide-area communications require substantially more attention to the design and implementation of threat detection and adaptable mitigation controls. Some adaptation and risk-management strategies and policies may reduce risk in the short term, such as with TLS, but may increase vulnerability and exposure over the longer term, such as the weaponization of TLS vulnerabilities and the subsequent field upgrades of TLS code.

ECS DSS device cyber vulnerabilities and exposure are largely related to Ethernet communications. Necessary Ethernet communications, such as pre-engineered and enabled file transfer, polling, and control capabilities that are protected by defense-in-depth strategies, should be considered necessary and not always a vulnerability. However, unnecessary but allowed communications capabilities that are not disabled are potential vulnerabilities to the system. Risk mitigation and adaptation practices will be most successful when they are both proactive in design and reactive in service to the dynamic nature of both vulnerabilities, as they evolve, and exposure while allowing the necessary capability to function. An example of proactive mitigation is to pre-engineer data flow to restrict authentication transactions so that they may pass only between the workstation and the relay station bus interface. Reactive mitigation would also deny authentication transactions on this isolated flow until they are dynamically enabled by an out-of-band control action by a third party. If the DSS communications architecture permits unintended use and manipulation of capabilities, they may represent vulnerabilities allowing exploits such as these:

1. Communications capabilities that are exploited or weaponized to allow espionage observation and analysis.
   (Espionage is used intentionally because no other word represents the reconnaissance, subterfuge, and data extraction which is often required before an interactive attack. Although the phrase commonly refers specifically to nation-states and nationalistic terrorists (those who have successfully attacked power delivery systems), it equally applies to internal and external actors that perform passive data monitoring as well as interaction.)
2. Authorization capabilities exploited to allow unauthorized interaction.
3. Message delivery capabilities that are exploited to allow espionage and false authorization.

TLS Version 1.2 was replaced by Version 1.3 in December of 2018, and then Version 1.3 was weaponized in February of 2019. Events like this illustrate the need to consider a feedback loop to evaluate added vulnerabilities associated with a mitigation control, such as Step 4 of the LVD in Section II. TLS is a popular secrecy mechanism created for internet-based commerce. However, vulnerabilities within it are frequently weaponized for use in attacks. Therefore, when added to ECS IEDs, TLS firmware will need to be updated in the field after a related, common vulnerabilities and exposures (CVE) notice is posted. If this new vulnerability must be corrected by remote firmware updates, this process may also be subsequently compromised. A more complete list of the challenges associated with adding the TLS e-commerce secrecy tools to end devices includes:

1. Complexity in key management.
2. Certificate creation that only lasts a certain amount of time and is not equal to the life of the system.
3. The increased complexity of getting encrypted versions of plaintext packets to an intrusion detection system (IDS) so that it can perform deep-packet inspection, thereby allowing the adversary to hide in legitimate traffic.
4. TLS is going to need to be replaced periodically owing to predicted advancements in quantum computing [11].
5. Quantum-safe cryptography ciphers will require hardware replacement for new trusted platform modules. These are generally not affordable for systems designed to last 15–25 years.

The SolarWinds event, in which attackers mimicked legitimate network traffic, avoided in-service threat detection methods, and distributed malicious code, illustrates the threats associated with field updates. Some mitigation controls therefore must be subsequently evaluated for the new threats that they represent, and if they are not addressed then the concatenating vulnerabilities become a vulnerability chain. A vulnerability chain represents the consequential threats added to the system due to the evolution of an existing vulnerability, new threats added by the vulnerability of mitigation controls, and the exploitation of the supply chain of potential corrective actions. For example, firmware upgrades to correct weaknesses in devices can enable attacks on all three security resilience concerns, including confidentiality, integrity, and availability [12].

IV. Example Threats to DSS Communications Capabilities

TLS provides message security through encryption, but even that capability can be exploited to allow espionage, observation, and analysis of the system. Version 1.3 was weaponized to allow an unauthenticated, remote attacker to bypass a configured TLS 1.3 policy in a firewall and block local-area network (LAN) traffic [7]. This is a remote attack which may happen at any time, and while the threat is constant the exposure only exists during remote communications to a process bus device. The impact varies based on what messaging is present during the attack. TLS is an example of a technology that is not primarily necessary to a system, but rather serves as a mitigation control to prevent attacks against necessary communications capabilities. TLS code can be replaced or updated in the field, but it is not adaptable to compensate for new threats while in service. However, tools like OT-SDN can reduce exposure after the attack or adaptively restrict data flows.

An example of an attack on the LAN message delivery capability that may allow espionage (and, in very rare events, false authorization) is the message delivery exploit performed by a man-in-the-middle or address resolution protocol (ARP) poisoning attack [13]. This attack may successfully capture authorization credentials if each of the following exposures and events exist.

1. Communications are unintentionally exposed via an undetected and unauthorized human intruder in the substation with an undetected computer connected to the LAN.
2. Internet protocol (IP) addresses are unintentionally exposed to an intruder successfully launching an ARP poisoning attack on the LAN switch which reroutes traffic traveling between a device and workstation through the undetected computer each direction.
3. IP messaging is unintentionally exposed to an intruder via undetected observation of IP addresses, and authorization credentials for R&W engineering access to the device is performed by a second authorized human who is unaware of the presence of the intruder.
4. An intruder is performing undetected use of credentials to connect to a device from an undetected LAN-connected computer.
5. An intruder is using previously gathered information about or from a device to control or reconfigure that device.
6. An intruder exits the substation undetected.

This is an espionage-enabled attack which can happen only after an attacker locally observes a password exchange initiated by an authorized local user, so the exposure is directly related to how often, if ever, a legitimate workstation-to-device authentication transaction is performed using the password command. The observed password must also be sufficient to gain R&W access control and device-configuration authorization. Therefore, the observation exposure is directly related to the likelihood of the legitimate local user initiating the device password command to gain R&W authorization to control or reconfigure the device from the workstation. If the utility does not permit R&W engineering access, the exposure to observation is zero. Otherwise, the exposure to observation is related to how often the engineering access is initiated, rather than the duration of the engineering access process. It is estimated that R&W engineering access authentication credentials are passed to each process bus device during a transaction lasting less than one minute every five years [9]. Additionally, the exposure is directly related to the likelihood of a second unauthorized human intruder's (and their LAN connection) unobserved presence.

Exposure via remote users is possible when the system allows a remote engineering workstation to connect across a wide-area public communications network, through a substation router, through the LAN, and to the device. In this case, a remote attacker may connect to the substation router via the public communication network and attack the router domain name server (DNS) function, or border gateway protocol (BGP), attack. These attacks may be successful to capture authorization credentials if each of the following exposures exist.

1. Communications are unintentionally exposed when an undetected and unauthorized remote human intruder successfully contacts the substation router via a public communications network.
2. The remote intruder successfully executes a DNS attack on the router to reroute traffic from between the substation device and the router, before it is encrypted, to a remote spoofing computer with an illegitimate DNS function.
3. Communications are unintentionally exposed via successful observation of an IP address and authentication credential transaction.
4. The return of traffic to the substation router where it is encrypted and then sent to the legitimate remote user.
5. Communications are unintentionally exposed when the remote intruder successfully connects, undetected, to the substation router and then to the substation device.
6. The undetected use of the credentials by the intruder to connect to a device from an undetected remote computer.
7. The undetected use of previously learned extensive knowledge of communications with the device to control or reconfigure the device.
8. The intruder's undetected exit from the substation.

This is an espionage-enabled attack which can happen only after a remote attacker observes a password exchange initiated by an authorized remote user, so the exposure is directly related to the likelihood of the appropriate remote-workstation-to-device password command. The execution follows the same steps as the ARP attack, but if the utility does not permit remote R&W engineering access, then the exposure to observation is zero. Additionally, the exposure is directly related to the likelihood of a remote R&W authorization transaction while a second, remote, unauthorized human intruder and spoofing DNS computer connection is present but unobserved.

Many process bus devices use IP Ethernet messaging for station bus R&W engineering access during configuration and commissioning, and occasionally during authenticated supervisory control and data acquisition (SCADA) commands. Some in-service devices support read-only engineering access for applications such as SCADA, event reports, diagnostics, synchrophasors, and process bus supervision. Many process bus devices use Layer 2 Ethernet (L2) messaging for machine-to-machine communications to the station bus, such as generic object-oriented substation event (GOOSE), sampled values (SV), and precision time protocol. These non-IP process bus protocols are not subject to the ARP poisoning and DNS attack scenarios.

V. Vulnerability Chain Example

It is difficult to manage mitigation controls (for instance, adding TLS secrecy to necessary communications capabilities) that can evolve into known vulnerabilities over time; for example, a common vulnerability disclosure (CVE) informs a user that their in-service version of TLS has become weaponized. After learning this, the system will require adaptation via the coordinated field updates of firmware in all client-server devices across the system. Adaptation via firmware upgrades is most difficult when inadequate device inventory management results in unknown distribution of weaponized TLS among in-service devices. Further, mitigation is impossible if there is no CVE to make the vulnerability known. This uncertainty and complexity make static capabilities (such as successfully protected passwords in the clear) a better choice because they are easier to predict and understand. The use of passwords in the clear to provides enough confidence that the in-service devices remain in a known and static cybersecure state, protected by defense-in-depth architecture choices, as the internet-based security technology constantly changes and evolves.

Using an event tree, two vulnerabilities that must simultaneously exist to allow a successful attack are combined via Boolean logic. However, a vulnerability chain considers the introduction of a new vulnerability as the unintended consequence of a mitigation control. For example, the MITRE ATT&CK framework reiterates that capabilities present in IEDs do not automatically create risk and do not permit direct and immediate attack. Intruders must gain access to the system, usually through an IT-to-OT connection or by hijacking a wide-area network (WAN) link between the control center and the substation, via the series of steps that include initial access, persistence, escalation, evasion, discovery, lateral movement, command and control, observation, and analysis of important data capable of impacting that specific system before the IED is exposed [3].

One weakness, such as the use of TLS secrecy, leads to a second weakness, the inevitable obsolescence of the presently used TLS cipher suite. This leads to yet another weakness such as the weaponization of TLS or simply a mismatch of versions in the field, which, in turn, leads to another weakness associated with the removal of devices from service for field updates of firmware. If done remotely, this may lead to yet another weakness by allowing malware to be introduced into the devices, as was done by the SolarWinds automatic push of malicious code. Vulnerability chains associated with a potential mitigation control can be modeled with ATA; however, it is important to recognize that they are a moving target as new weaknesses are frequently being added or recognized.

Capabilities such as IP messaging with DSS devices via plaintext remain uncomplicated and effective. These capabilities are easily initially and adaptively protected via processes that limit or eliminate R&W access via utility processes and/or OT-SDN flow control. Further, they can be enhanced by automatic password rotation and passing the communications through a real-time controller that acts as a message proxy, protocol break, or condition monitor. Additionally, remote communications are enhanced by passing through a security gateway and firewall. Lack of secrecy also permits traditional LAN cybersecurity methods, malware detection, IDS, intrusion prevention system (IPS), and the security information and event manager. Vulnerability chains develop based on the choice of mitigation control and not the capability itself.

VI. Cyber Vulnerability Assessment Applied to Digital Secondary Systems Using an Attack Tree

An ATA is a graphical visualization method capable of measuring cyberthreats of a cybernetic system [14] [15]. 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 is constructed using the ETA method focusing on cyberthreats, and it relies on the knowledge of device and system vulnerabilities. The results may be used as a leaf on another event tree and could include the exposure and consequences of each vulnerability, such as service outage or data loss, and the consequences of proactive and reactive mitigation controls. Those results may then be used as leaves of another event tree to investigate the ramifications of choosing dynamic solutions (such as TLS), the interdependencies of installation and O&M costs, and the benefits of mitigation controls.

However, as with all event trees, not all leaves have the same impact, and the weight of individual cyberthreats is not well understood. This paper introduces metrics and methods to predict the risk of individual cyberthreat events so that they can be used to understand and manage risks to a whole system as well as to specific substation installations.

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 for 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.

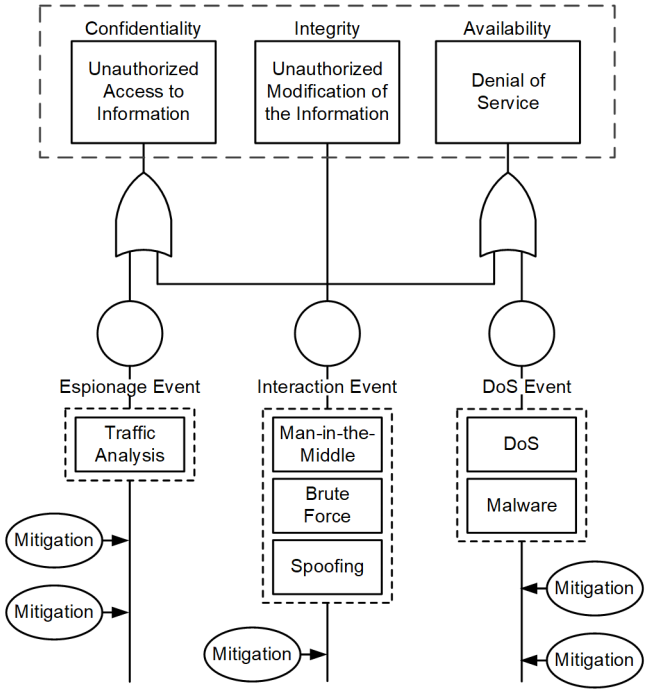

Fig. 1. Attack tree applied to DSS

In sequence, the root nodes are decomposed into several subtasks representing cyberattack threat events, and mitigation leaves characterized countermeasures. Three major events are identified for this attack tree: espionage, interaction, and denial-of-service (DoS) events. Based on its trait characteristics, each event type contributes to compromising the CIA index in some way. Note that some events can contribute to the degradation of more than one index; the next sections present the definitions used to decide each attack event's scope in the proposed attack tree modeling.

A. 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 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 WAN, may use secrecy to hinder espionage outside the LAN perimeter. This uncomplicated password-based user authorization may be vulnerable to espionage if LAN traffic is observed, or if secrecy, such as encryption, is not added before it is routed out of the substation. Due to the design and capability of each device, most remote access sensitive information, such as passwords and SCADA information, is exchanged with devices on the station bus in a DSS. Because of this property, remote-access espionage events will only impact DSS process bus devices if the process and station bus are connected. Though unlikely, espionage events of local and remote communications contribute directly to the degradation of the confidentiality index.

B. 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. Other common interaction techniques include man-in-the-middle attacks, BGP attacks, Remote Desktop protocol attacks, brute-force attacks, and spoofing attacks. Though it is possible to detect the effect of these attacks and adapt logic in the process bus devices, the attacks are sporadic and difficult to observe because of their complex execution. Though they are sporadic and unpredictable, many interactive events first require espionage to learn authorization and operational details. However, if the attack is successful, then it could introduce extreme danger to the electric power system, like the power outages in the Ukraine cybersecurity events of 2015 and 2016 [16]. Therefore, interaction events will be considered a common degradation entity to all the root nodes' indexes.

C. DoS Events

The goal of 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 [17]. DoS attacks can be detected by IDS and IPS systems and can be detected and controlled through OT-SDN. However, considering that the DSS's data rate, by nature, has a high number of messages that requires high-speed delivery and little jitter, IPS real-time packet inspection techniques may be ineffective at prevention or compromise the DSS's performance and reliability. In this case, DoS events contribute directly to the degradation of the attack tree's availability node.

D. 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:

- Encryption and authentication
- Network architecture

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. However, data encryption alone is not sufficient to keep the system safe; in some situations, like the replay attacks, the attacker can replay encrypted data through the network and force the receiver to respond to those bad packets [18] [19]. Therefore, another layer of security is necessary. Usually, encryption comes with authentication: a secure footprint tag process used to authenticate the messages' sender.

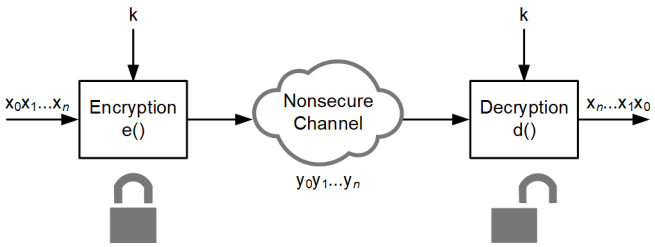

Fig. 2. Encryption and decryption functions

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 because of 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 SV. Therefore, encryption solutions can be a drawback to the system's performance, even unacceptably so. However, there is an effort from the community to mitigate this latency performance issue, and some tools are available to reduce the key rotation management process [20] [21] [22].

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 [23]. 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 OT-SDN [24] [25]. 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 [26]. 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.

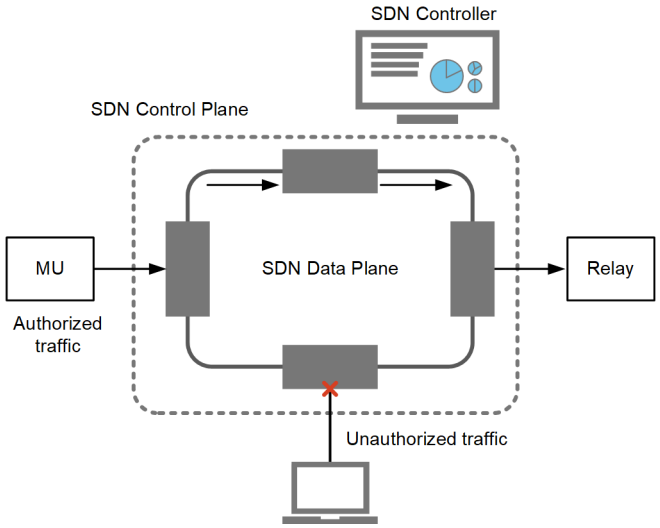

Fig. 3. OT-SDN

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 standard has a variety of network designs applied to the process bus, such as point-to-point, duplicated star, single ring, etc.; refer to [27] [28] [29] [30]. However, DSSs have a unique challenge due to the real-time nature and volume of traffic. In most 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.

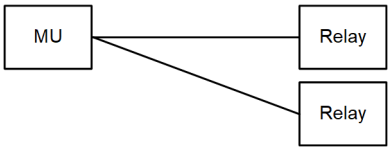

Fig. 4. Point-to-multipoint DSS architecture

VII. 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 [31]. 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.

A. Threat Availability (TA)

The threat availability leaf index *TA* 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) .

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

The first part of the equation is the vulnerability score (VS), which represents the severity of the exploited vulnerability. One way to calculate this is to take the CVSS score system originally intended for IT and adapt it for use in OT systems. The CVSS is an open framework metric tool managed by NIST and used as a standard score to measure cyber systems' 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 considered the base CVSS score vector as described in Table XIII. The explanation of each score field is out of the scope of this paper and can be found in [32].

Each attack leaf has a VS score based on the attack exploitability and impact metrics. For example, in the "sniffing station bus protocol" attack situation at Table XIV, the VS vector is AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N, which is detailed as:

- Attack Vector (AV): Network
- Attack Complexity (AC): Low
- Privileges Required (PR): None
- User Interaction (UI): None
- Scope Change (S): Unchanged
- Confidentiality Impact (C): High
- Integrity Impact (I): None
- Availability Impact (A): None

The attack vector is computed based on the level of severity of each vector chosen, and the example above scores a total of 7.5.

The second component of (1) is the operational electrical substation metric measured in the power outage hours, resulting in a successful cyberattack.

Tables XV–XVII in the Appendix describe the vulnerability considerations for each case chosen and their applicable buses. The last column represents the logical combination of attack vectors used in the NIST CVSS calculator. Therefore, the index *TA* is a measure of the threat availability, or severity of the system's vulnerability tailored to a cyber occurrence event in an electric substation environment.

B. Cyber Mitigation of Leaf (Ω)

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

$$\Omega = \mathrm{Resilience} - \mathrm{Complexity} \quad (2)$$

Each of the equation installments has a low, medium, or high weight value, as shown in Table I. 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 I
Cyber Mitigation Weights Levels

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

For the Ω levels in this case study, a system resilience = 0 represents the most vulnerable system, and resilience = 10 is the least vulnerable system. According to the Presidential Policy Directive 21, resilience for the power grid is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions" [33]. 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 TLS cipher suites; Table II shows the cipher suite's situation awareness [34]. The obsolete ciphers have known public vulnerabilities released, which means they are not secure anymore and are no longer considered computationally safe. A cipher is considered computationally safe for the period of time in which the best-known attack method is by key exhaustion (brute force). It is a delicate balance to promote a cipher that is computationally complex enough to be safe but not so complex as to be efficiently deployed in devices. However, by design, it is inevitable that as computational capability in the market grows, older cipher mitigation methods with known vulnerabilities will become unsafe with low resilience levels. But Advanced Encryption Standard (AES) is still safe and can be considered to have high resilience levels. The same methodology will apply along with the other resilience mitigation leaves chosen for this paper and will be further discussed in the next sections.

Table II
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 [35]. 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 third-factor authorization of the R&W access control, then it can act as the low-complexity authentication process providing a high level of resilience against interaction events. Table XVIII in the Appendix summarizes the resilience and complexity levels chosen for this experiment and the applicable buses.

C. CIA Root

Equations 3–5 are derived by the attack tree shown in Fig. 1.

$$C_{root} = \left(TA_{espionage} - \Omega_{confidentiality}\right) + \left(TA_{interaction} - \Omega_{integrity}\right) \quad (3)$$

$$I_{root} = \left(TA_{interaction} - \Omega_{integrity}\right) \quad (4)$$

$$A_{root} = \left(TA_{Dos} - \Omega_{availability}\right) + \left(TA_{integrity} - \Omega_{availability}\right) \quad (5)$$

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.

VIII. DSS Security Network Architectures

The DSS process bus extends the substation yard to the control house over a communication network that defines the security boundary line between the primary equipment and the protection and control system. This section presents three DSS process bus topology variants and compares and contrasts their cyber vulnerabilities. Each of these topologies has the same station bus architecture: a switched-Ethernet LAN connected to an engineering workstation, a local SCADA, and a substation router. In addition, it uses the applied R&W access control mechanism to secure station bus networks.

A. Point-to-Point Architecture

Using a point-to-point architecture in the process bus keeps the relay as the main component for the protection system, as shown in Fig. 5. The point-to-point architecture organically segregates the protection signals from the automation and SCADA network. This function is referred to as a protocol break because the relay logically separates the process and station bus communications. This property is a natural barrier against cyberthreats and provides good cybersecurity resilience: the attacker needs physical access to the site to tamper with the merging unit (MU) data or connections. In this case, the relay acts as a protocol break to isolate the process bus protocols from the station bus.

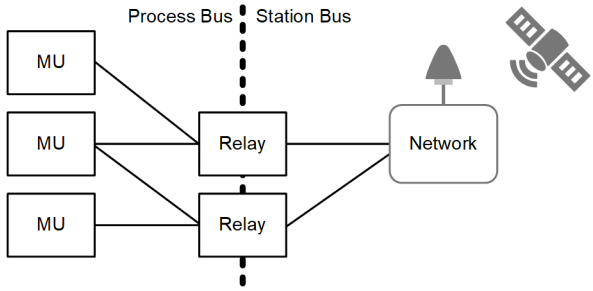

Fig. 5. Point-to-point architecture

Another advantage of the point-to-point architecture is that time synchronization is not required to exchange protection and control signals. To make data coherent from multiple MUs only requires relative time between the devices. Because point-to-point connections have a fixed latency, the subscribing relay can calculate latency using a ping-pong method and compensate for each channel's latency. In this way, the subscribing device acts as a de facto time source.

To meet the flexibility needed for practical applications, many modern MUs that use point-to-point connections feature multiple ports, allowing the MU to share data with multiple relays while maintaining the point-to-point architecture advantages.

Fig. 6 shows the MU's capability of receiving control signals from the process bus interfaces. The signals are verified by virtue of their source, making the verification a straightforward way of handling control signals, thus making them easier to implement and, therefore, less prone to human error. The potential vulnerability of an intruder connecting to an unused signal path is minimal because physical access would be required, and the device would need to be reconfigured to accept the new communication link. Hijacking an existing commissioned link is equally unlikely because it requires physical access to the MUs; the loss of communications during the cable reconfiguration would be detected. Simple logic in the MU may be implemented to prevent control commands from a link with a suspicious outage until the logic is reset by a third party. Also, to take advantage of a hijacked link, the intruder control signal source would need to be developed to understand and communicate with the specific point-to-point protocol. And so, the physical security measures at a substation effectively become the cybersecurity measures to this particular vulnerability [36].

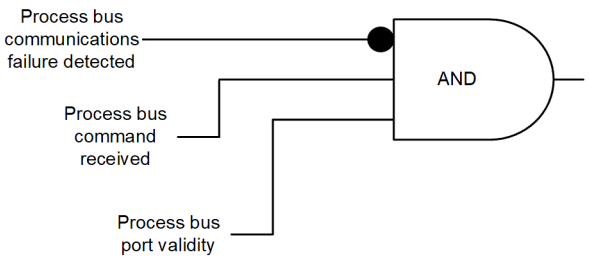

Fig. 6. MU control

In addition, modern MUs needed to be submitted to cyber laboratory testing, such as fuzzer testing [37] [38]. Fuzzing is a DARPA-approved technique used to perform test and evaluate the cyber resiliency of typical communications methods. However, due to these unique devices' time-critical nature, the majority of MUs have a consecutive packet timing security check implemented, making it harsh to use standard and commercial fuzzer tools. Therefore, a unique real-time fuzzer technique is needed to guarantee the fuzzer test results.

B. Network-Switched Process Bus

Another possible process bus layout is an Ethernet multicast network with traditional Ethernet switches dedicated to the process bus, as shown in Fig. 7, but with no connection to the station bus. Due to a multicast network's highly versatile nature, the DSS system layout is essentially infinitely configurable. However, the DSS static characteristics usually do not require that level of flexibility and can be limited to pre-engineered functions to reduce the cyberattack surface.

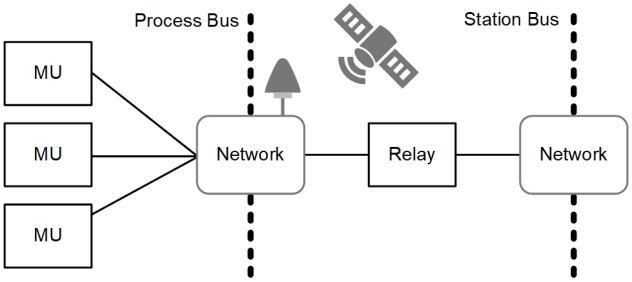

Fig. 7. Dedicated network-switched process bus

Similar to the point-to-point architecture, using a dedicated network for the process bus segregates protection signals from automation and SCADA networks and provides a natural barrier to attacks that use those channels.

Multicast packet traffic on the process bus, including SV and GOOSE messages, require IEEE 802.1 message delivery methods such as VLAN tags for better network segregation, because the large amount of traffic on an unmanaged network may quickly overwhelm unprepared connected devices and an unmanaged network presents a large cybersecurity risk. If malicious actors were to access an unmanaged network by physically accessing a spare LAN port or the WAN to do the same, then they may gain access to all data and end devices on the process bus. Further, they may be able to inject messages onto the process bus which, if the LAN is not configured to filter message delivery, could adversely affect the devices. This represents an unacceptable security risk, and while the use of unique VLANs on each multicast message header, with no other mitigations, is necessary, that alone would not be a sufficient solution. Therefore, VLANs represent one part of a larger cybersecurity posture needed for process bus applications.

In a switched-Ethernet DSS process bus, a system-wide time-synchronization reference is needed to connect multiple MU sources. Since a switched network is not symmetric, may change latency after fault correction, and does not guarantee a fixed jitter, the common time reference is used to record the samples in the publisher and then align the samples in the subscriber relay. Therefore, time-synchronization exploits such as GPS signal jamming and time-synchronization protocol attacks are a cyberthreat to DSSs [39].

Like the point-to-multipoint solution, the multicast messaging over the LAN supports control actions from multiple publishers. This adds complexity to the configuration of the system in exchange for a more flexible choice of signal sources. However, using this method, the MU will need to filter and identify incoming messages to confirm that they are valid. This adds complexity to the configuration of the system in exchange for a more flexible choice of signal sources, allowing the user to freely implement as complex or simple a scheme as desired. Part of this consideration should include a cybersecurity assessment of the complexity of the code necessary to evaluate the validity of a control message and how this may compromise the cybersecurity of the system.

It is also assumed that the best practice of not excessively overbuilding the network is in place to minimize the cyberattack surface and reduce the chances of an error in programming occurring.

C. OT-SDN Process Bus

Using an OT-SDN solution for the packet-based switched-Ethernet process bus is similar to the multicast Ethernet network in the physical configuration. Because of the deny-by-default architecture, it allows intrinsic cybersecurity for the communications system. DSS is a static architecture that hardly changes, and OT-SDN naturally provides the infrastructure needed to allow only the pre-engineered data flow into the LAN, and then block, quarantine, and raise the alarm for unrecognized internal and external traffic. The pre-engineered data flow rules are designed and configured in the control plane and the messages travel only to predetermined destinations at line speed on the data plane, as shown in Fig. 8.

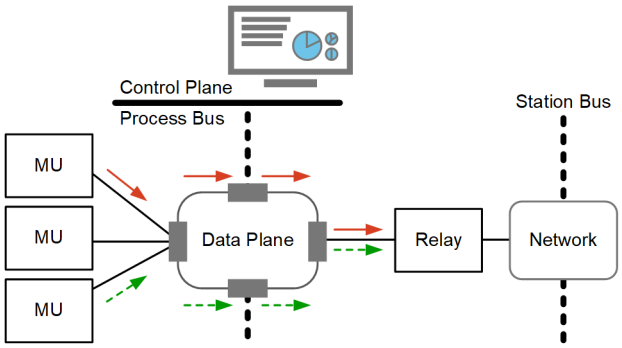

Fig. 8. OT-SDN process bus and network-switched station bus

The control plane is the central configuration application that supports the configuration of a pre-engineered set of rules (flows) and network visualization. In OT-SDN, the controller uses a secure connection through an open protocol, such as OpenFlow, to allow configuration of border devices, such as switches [40]. OT-SDN does not require that the controller be connected during the network operation; it is only needed during commissioning or for network-awareness purposes.

The data plane is where the equipment receives instructions from the controller and forwards the packets to their respective destinations. Unexpected packets are discarded or sent to an

IDS. The OT-SDN switches store the flow rules in flow tables, and the list of flow entries consists of predefined match-field values and actions. Therefore, the only traffic allowed to the OT OT-SDN network is configured in advance through a precise engineering process, providing real-time packet evaluation and intrusion prevention. That is where OT-SDN cyber resilience dwells.

Usually, OT-SDN has the ability to match any field from the Open System Interconnection (OSI) Layers 1–4. In DSSs, most of the traffic is composed of OSI Layer 2 packets. Therefore, there is no need to maintain OSI Layer 3 and Layer 4 packets flowing in the infrastructure, reducing the cyberattack surface. For that reason, OT-SDN is considered a high-resilience solution for cybersecurity problems.

D. R&W Access Control

R&W access control is a more straightforward solution that does not require a local cryptosystem infrastructure to operate. The idea is to use the relay functionality to lock itself in read-only operation most of the time and only grant local and remote write operations when an audited third-party entity allows it. Fig. 9 shows an example of the R&W access control through the SCADA system.

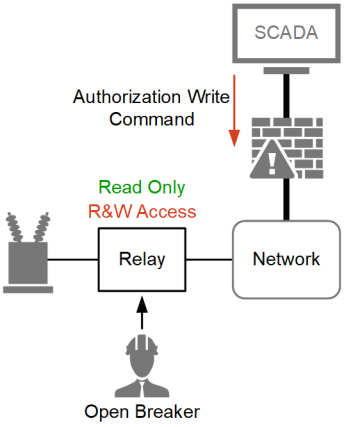

Fig. 9. R&W relay control access

The SCADA system is connected to the substation network through a secure connection and is a trusted and audited entity to the relay. If a user needs to open the breaker through the relay, then the relay will need further writing authorization from the SCADA system to operate the breaker. Once the breaker maneuver is done, the SCADA system can return the relay to read-only mode.

Another aspect is that an electric substation is a controlled environment with predefined physical- and cyber perimeters. Therefore, data confidentiality can be achieved within these premises. Since the predefined substation perimeters carry on confidentiality, the R&W access control can add an additional layer to cybersecurity integrity and availability properties.

IX. DSS Cybersecurity Vulnerability Assessment Evaluation

This section will evaluate two scenarios with a total of six cases to illustrate the use of threat availability analysis to compare and contrast design choices. The first scenario will consider 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

The second scenario will consider a common point-to-point process bus and three different station bus architectures:

- Case 4: traditional network with cryptography
- Case 5: traditional network with R&W access control
- Case 6: OT-SDN station bus

A. Scenario 1: Cyber Evaluation of DSS Process Bus Architectures

In all three case study architectures, the relays are connected to the station bus for engineering access and 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 DSS solutions.

1) Station Bus TA Leaves

Table III represents the *TA* values for each of the station bus communication types:

- Sniffing station bus protocols
- Interaction events with SCADA system, such as man-in-the-middle attacks
- Brute-force attacks
- DoS malware
- Read-only engineering access exploitations
- R&W engineering access exploitations

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 III
CYBERATTACK LEAVES RESULTS FOR STATION BUS COMMUNICATIONS BUS

Case 1	$TA_{Espionage}$	$TA_{Interaction}$	TA_{DoS}
Sniffing station bus	7.5	x	x
SCADA	x	13.4	x
Brute-force attack	x	6.3	x
Station bus malware	x	0	7.5
Read-Only Engineering Access	x	5.1	x
R&W Engineering Access	x	12.2	x
TA_{Total}	7.5	37	7.5

2) Total Cyberattack Leaves

Table IV–VI 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 IV
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 V
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 VI
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**

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 VII–IX show the process bus mitigation leaf values from Cases 1–3.

TABLE VII
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 VIII
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 IX
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) CIA Indexes Results

Fig. 10 shows the results from the CIA VS according to (3)–(5) as applied to each of the three process bus topologies.

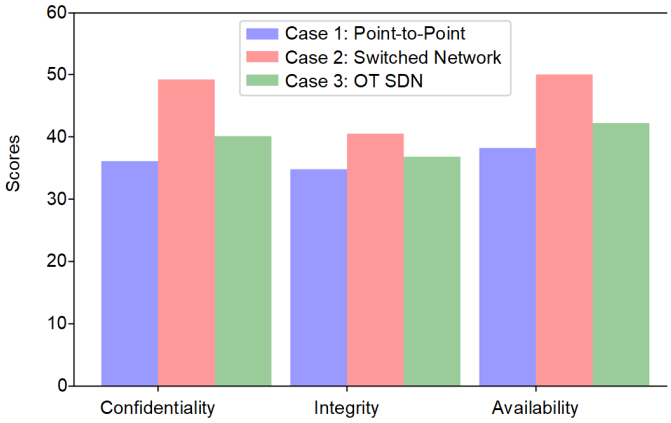

Fig. 10. CIA vulnerability scores for Cases 1–3 using station bus traditional networking and cryptography

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 X displays the improvement, over Case 2, of the relative cybersecurity threat availability scores for DSS Case 1 and Case 3.

TABLE X
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%

Table X 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 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.

B. *Scenario 2: Cyber Evaluation of DSS Station Bus Architectures*

This section explores different station bus architectures, each with the same fixed point-to-point process bus solution.

1) *Station Bus Cyberattack Leaves*

The attack leaves for the station bus are the same as the previous case and are described in Table III.

2) *Total Cyberattack Leaves*

The total cyberattack leaves for Cases 4–6 are described in Table IV and are considered the same.

3) *Cyber Mitigation Leaves*

The cyber mitigation leaves for Cases 4– 6 are shown in Table XI–XIII.

TABLE XI
CASE 4: MITIGATION LEAVES VALUES FOR POINT-TO-POINT PROCESS BUS AND STATION BUS WITH CRYPTOGRAPHY

Case 4	$TA_{Confidentiality}$	$TA_{Integrity}$	$TA_{Availability}$
Station Bus	3	2	1
Process Bus	7	7	7
TA_{Total}	**10**	**9**	**8**

TABLE XII
CASE 5: MITIGATION LEAVES VALUES FOR POINT-TO-POINT PROCESS BUS AND STATION BUS WITH R&W ACCESS CONTROL

Case 5	$TA_{Confidentiality}$	$TA_{Integrity}$	$TA_{Availability}$
Station Bus	0	9	7
Process Bus	7	7	7
TA_{Total}	**7**	**16**	**14**

TABLE XIII
CASE 6: MITIGATION LEAVES VALUES FOR POINT-TO-POINT PROCESS BUS AND OT-SDN STATION BUS

Case 6	$TA_{Confidentiality}$	$TA_{Integrity}$	$TA_{Availability}$
Station Bus	5	5	5
Process Bus	7	7	7
TA_{Total}	**12**	**12**	**12**

4) *CIA Indexes Results*

Fig. 11 shows the results from the CIA vulnerability indexes according to (3)–(5).

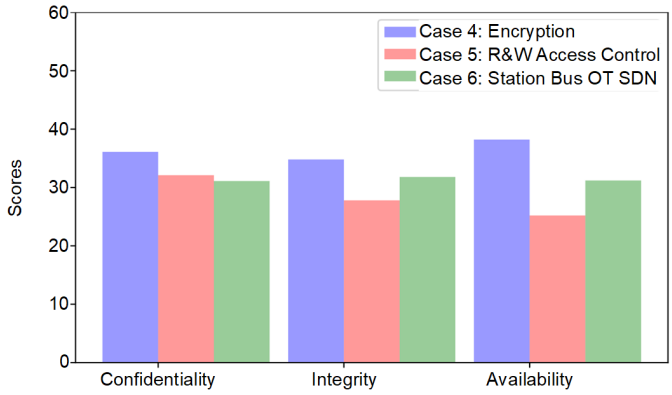

Fig. 11. CIA vulnerabilities scores for Cases 4, 5, and 6

The results show that the highest scores—and the highest threat availability—are always associated with Case 4, the traditional switched network. Table XIV displays the reduction of cybersecurity threat availability scores for both Case 5 and Case 6 relative to the results of Case 4.

TABLE XIV
CYBERSECURITY IMPROVEMENT RELATIVE TO CASE 4

Station Bus Architectures	**Relative Improvement**		
	C_{Root}	I_{Root}	A_{Root}
Case 5: R&W	11%	20%	34%
Case 6: OT-SDN	13%	8%	18%

In addition to being uncomplicated, R&W access control shows a good balance between security and complexity and is a suitable candidate for DSS implementations. Though low, the increased threat availability of OT-SDN is related to the required pre-engineering and potential for misuse of legitimate data flows. Of course, combining OT-SDN with access control creates a far superior solution with no negative performance impacts on the process bus.

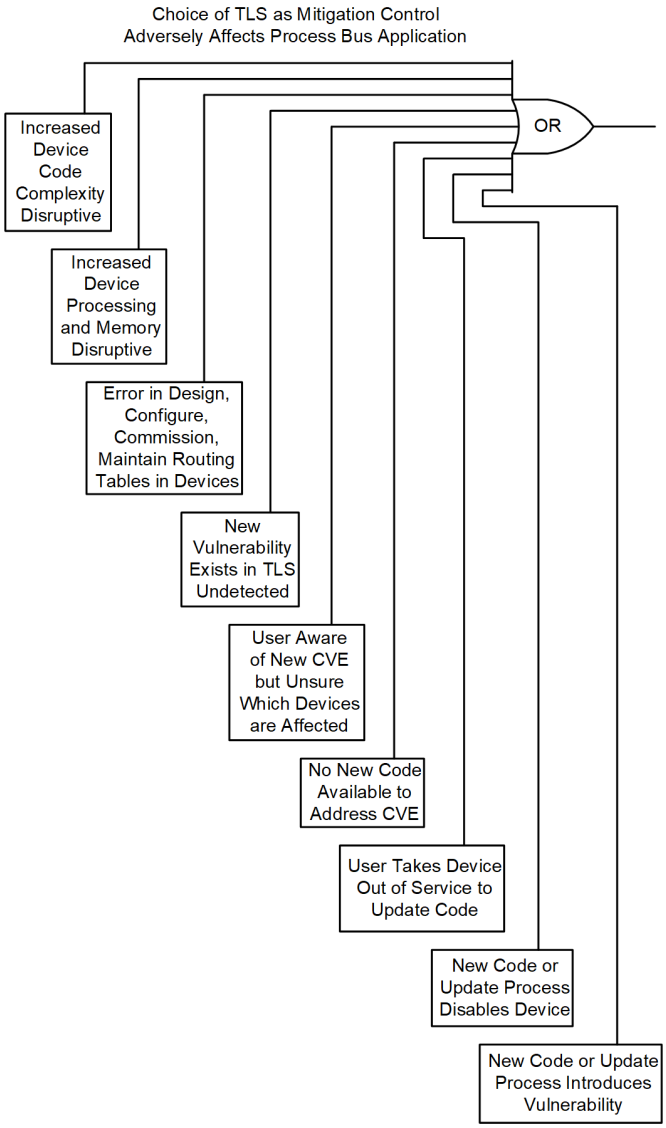

Fig. 12. ETA with top event of disruption to process bus application due to use of TLS

Fig. 11 shows that secrecy as a mitigation control does not materially change the vulnerability of station bus designs. However, when the vulnerability chain of TLS is considered, the station bus applications become much more vulnerable. ETA provides a useful way to understand the vulnerability chain of unintended consequences. For example, since the internet engineering task force first created TLS to secure commercial transactions performed over the internet, it has been updated numerous times to correct vulnerabilities. Version 1.2 addressed several vulnerabilities in the previous version, and then Version 1.3 was released by the IEFT in March 2018, to address vulnerabilities in 1.2. In December of 2018, NIST required that devices be upgraded to Version 1.3,and then in February 2019, a new vulnerability in 1.3 was recognized. CVE-2020-3285 documents how this vulnerability was quickly weaponized, and thus needed to be corrected with new code. This means that TLS firmware needed to be updated in field devices twice within the span of three months.

When cryptography via TLS is chosen for the station bus, it introduces each possible negative unintended consequence, as illustrated in Fig. 12. This ETA considers all of the possible contributors to a disruption of the process bus applications as event tree branches. A Boolean OR gate is used because each leaf represents an individual threat.

X. Analyzing the Impact of Exposure

A capability, such as local R&W engineering access to change or control a process bus relay, is only vulnerable if it is exposed to a potential threat. In this example, the capability to authenticate a user is kept uncomplicated by the exchange of passwords as plaintext acting as tokens. There is no risk of observation if R&W engineering access is disabled. Otherwise, the ETA for exposure follows Boolean logic, as in Fig. 13, including the following:

1. The exposure to observation, limited to the duration of the authentication transaction which is typically one minute each five years.

AND

2. The exposure to observation, further limited to the spoofing of a pre-engineered OT-SDN dataflow.

AND

3. The exposure to observation, further limited to a situation in which the observation and intruder remaining undetected and exiting the substation undetected.

AND

4. The exposure to interaction, limited to the period of time until the password is automatically changed by the security appliance, perhaps the duration of the existing month.

AND

5. The exposure to interaction, further limited to the point in time when the third factor authorization performs R&W engineering access control.

AND

6. The exposure to interaction, further limited to the spoofing of a pre-engineered OT-SDN dataflow.

AND

7. The exposure to interaction, further limited to the point in time when the third factor authorization performs R&W engineering access control.

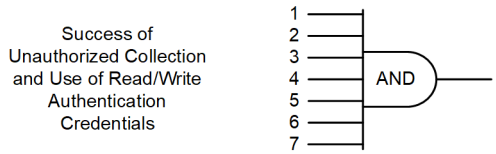

Fig. 13. ETA with top event of unauthorized use of R&W engineering credentials

Unlike encryption, engineering access control has no vulnerability chain and the exposure is low. Using OT-SDN on the station bus further reduces the exposure of the authentication transaction. Plaintext passwords used as tokens are interoperable with any engineering tool software and avoid secrecy on the station bus; however, there may be hidden malware and control attacks on the station bus. Using a functional access control instead of encryption makes the

solution static and unchanged while internet security methods evolve, which provides confidence that it will remain uncomplicated and predictable. This lack of new firmware, when set against other devices' need to update firmware as vulnerabilities evolve, dramatically reduces operation and maintenance costs.

XI. Conclusion

The LVD concept describes an interactive approach to identify and mitigate system design gaps based on cost, schedule, and performance. The goal for an ECS is to create an infrastructure designed to detect accidental and intentional, physical and cyber, employee and terrorist threats, to isolate resulting damage, and to promote the survival of personnel and equipment affected by an event, while propagating continued use of the infrastructure. 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. It is common to design for hardware availability of ECS by evaluating the reliability and maintainability based on mean time to detect and MTBF information. MTBF provides a comparison of the unavailability to serve among different component choices. Previously, the comparison of cyberthreats was not possible due to the lack of a universal comparison metric. 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 for 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.

The second evaluation analyzed a variant for the station bus mitigation leaf, the R&W access control is a simpler and more efficient variant approach to be applied in a controlled environment, such as a substation. The point-to-point DSS case was used to compare the encrypted station bus solution against the R&W access control variant. The results showed that the R&W access control has a good balance between complexity and security and is a valid option if encryption and authentication are not required.

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 introduces a methodology to help design engineers to understand and explore this weakness before deploying these systems.

XII. Appendix

TABLE XV
ANALYSIS EVENTS CYBER INDEX

Espionage Events	Buses	CVSS	Power Outage (Hours)	TA_{Leaf}	CVSS v3.1 Vectors
Sniffing Station Bus Protocols	Station	7.5	0	7.5	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Sniffing Process Bus Multicast Network-Switched	Process	6.2	0	6.2	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Sniffing OT-SDN Process Bus	Process	3.8	0	3.8	AV:P/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N
Sniffing Process Bus Point-to-Point Architecture	Process	3.8	0	3.8	AV:P/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N

TABLE XVI
INTERACTION EVENTS CYBER INDEX

Interaction Events	Buses	CVSS	Power Outage (Hours)	TA_{Leaf}	CVSS v3.1 Vectors
Man-in-the-Middle Attack	Station	7.3	5	12.3	AV:A/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H
Brute-Force Attack	Station	6.3	0	6.3	AV:A/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:L
Spoofing Process Bus Multicast Network-Switched	Process	7.5	5	12.5	AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H
Spoofing OT-SDN Process Bus	Process	6.8	5	11.8	AV:P/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H
Spoofing Process Bus Point-to-Point Architecture	Process	6.8	5	11.8	AV:P/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H

TABLE XVII
DOS CYBER INDEX

DoS Events	Buses	CVSS	Power Outage (Hours)	TA_{Leaf}	CVSS v3.1 Vectors
Station Bus Malware	Station	7.5	0	7.5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Malware Process Bus Multicast Network Architecture	Process	5.0	0	5.0	AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H
Malware Process Bus OT-SDN	Process	3.9	0	3.9	AV:P/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H
Malware Process Bus Point-to-Point Architecture	Process	3.9	0	3.9	AV:P/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H

TABLE XVIII
MITIGATION CYBER INDEX

Mitigation	Buses	Resilience			Complexity	Ω Total		
		Confidentiality	Integrity	Availability		Confidentiality	Integrity	Availability
Cryptography (Encryption and Authentication)	Station	10 (high)	10 (high)	10 (high)	7 (high)	3	3	3
R&W Access Control	Station	1 (low)	6 (medium)	3 (low)	1 (low)	0	5	2
VLANs	Process	5 (medium)	5 (medium)	5 (medium)	3 (low)	2	3	3
OT-SDN	Process	10 (high)	10 (high)	10 (high)	5 (medium)	5	5	5
Point-to-Point	Process	10 (high)	10 (high)	10 (high)	3 (low)	7	7	7

XIII. References

[1] G. W. Scheer and D. Dolezilek, "Selecting, Designing, and Installing Modern Data Networks in Electrical Substations," proceedings of the Relay Protection and Substation Automation of Modern EHV Power Systems, Cheboksary, Russia, September 2007.

[2] D. Dolezilek, P. Lima, G. Rocha, A. Rufino, and W. Fernandes, "Comparing the Cost, Complexity, and Performance of Several In-Service Process Bus Merging Unit Solutions Based on IEC 61850," proceedings of the 15th International Conference on Developments in Power System Protection, Liverpool, United Kingdom, March 2020.

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

[4] S4 Events, "A New CVSS for ICS Vulnerabilities," accessed January 26, 2021. Available: youtu.be/-6cThOCm9co.

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

[6] Department of the Army, "Utility Systems Terrorism Countermeasures for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities," February 2006.

[7] CVE, "CVE-2020-3285," accessed January 21, 2021. Available: cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3285.

[8] Crowdstrike Intelligence Team, "SUNSPOT: An Implant in the Build Process," accessed January 21, 2021. Available: crowdstrike.com /blog/sunspot-malware-technical-analysis.

[9] J. Kumm, M. Weber, E.O. Schweitzer III, and D. Hou, "Philosophies for Testing Protective Relays," proceedings of the 48th Annual Georgia Tech Protective Relaying Conference, Atlanta, GA, May 1994.

[10] The President's National Security Telecommunications Advisory Committee, "Draft NSTAC Report to the President on Software-Defined Networking," accessed January 26, 2021. Available: cisa.gov/sites/default/files/publications/Draft%20NSTAC%20SDN%20Report%20%287-28-20%29%20v2.pdf.

[11] B. Harris, "This is the biggest risk we face with AI, by Google CEO Sundar Pichai," January 23, 2020. Available: weforum.org/agenda/2020/01/this-is-how-quantum-computing-will-change-our-lives-8a0d33657f.

[12] C. Konstantinou and M. Maniatakos, "Impact of Firmware Modification Attacks on Power Systems Field Devices," New York University, 2015.

[13] MITRE ATT&CK, "Man-in-the-Middle: ARP Cache Poisoning," accessed January 21, 2021. Available: attack.mitre.org/techniques/T1557/002.

[14] N. Ferguson, B. Schneier, and T. Kohno, Cryptography Engineering: Design Principles and Practical Applications, Wiley Publishing, Inc., Indianapolis, IN, 2010.

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

[16] D. Whitehead, K. Owens, D. Gammel, and J. Smith. "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies," proceedings of the 43rd Annual Western Protective Relay Conference, Spokane, WA, October 2016.

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

[18] C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners," Springer, New York, NY, 2010.

[19] D. Whitehead and R. Smith, "Cryptography: A Tutorial for Power Engineers," proceedings of the 35th Annual Western Protective Relay Conference, Spokane, WA, October 2008.

[20] IEC 62351-6:2020, Power Systems Management And Associated Information Exchange - Data and Communications Security - Part 6: Security for IEC 61850, 2020.

[21] K. Boateng and A. Lashkari, "Securing GOOSE: The Return of One-Time Pads," proceedings of the International Carnahan Conference on Security Technology, Chennai, India, October 2019.

[22] D. Dolezilek, "Methods for Securing Substation LAN Communications," proceedings of the 5th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2003.

[23] S. M. Hussain, T. Ustun, and A. Kalam, "A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges," IEEE Transactions on Industrial Informatics, Vol. 16, No. 9, September 2020, pp. 5,643–5,654.

[24] M. van Rensburg, D. Dolezilek, and J. Dearien, "Case Study: Using IEC 61850 Network Engineering Guideline Test Procedures to Diagnose and Analyze Ethernet Network Installations," proceedings of the PAC World Africa Conference, Johannesburg, South Africa, November 2015.

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

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

[27] D. Dolezilek, J. Dearien, A. Kalra, and J. Needs, "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.

[28] S. Chelluri, D. Dolezilek, J. Dearien, and A. Kalra, "Design and Validation Practices for Ethernet Networks to Support Automation and Control Applications," proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2014.

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

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

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

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

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

[34] 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.

[35] J. D. Bewley, R. Zhang, T. Charton, and R. Wilson, "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, December 2020.

[36] NERC Standard CIP-006-6 - Cyber Security - Physical Security of BES Cyber Systems. Available: nerc.com/pa/Stand/Reliability%20Standards/CIP-006-6.pdf.

[37] T. Tu, H. Zhang, B. Qin, and Z. Chen, "A Vulnerability Mining System Based on Fuzzing for IEC 61850 Protocols," proceedings of the 5th International Conference on Frontiers of Manufacturing Science and Measuring Technology, Taiyuan, China, June 2017.

[38] Y. Yang, H.T. Jiang, K. McLaughlin, L. Gao, Y.B. Yuan, W. Huang, and S. Sezer, "Cybersecurity Test-Bed for IEC 61850-Based Smart Substations," proceedings of the IEEE Power & Energy Society General Meeting, Denver, CO, July 2015.

[39] M. Han and P. Crossley, "Vulnerability of IEEE 1588 Under Time-Synchronization Attacks," proceedings of the IEEE Power & Energy Society General Meeting, Atlanta, Georgia, August 2019.

[40] Open Networking Foundation. Available: opennetworking.org.

XIV. BIOGRAPHIES

Mauricio Gadelha da Silveira is an electrical engineer with a BS earned from São Paulo State University in 2013. Since 2014, he has been with Schweitzer Engineering Laboratories, Inc. (SEL), where he has held positions in SEL Engineering Services, Inc. (SEL ES), Sales and Customer Service, and R&D. He is currently a lead integration and automation engineer. His work includes development of protective relay protocols and communications, network design for critical infrastructures, power system modeling, and cybersecurity assessment.

David Dolezilek is a principal engineer at Schweitzer Engineering Laboratories, Inc. (SEL), and has three decades of experience in electric power protection, automation, communication, and control. He develops and implements innovative solutions to intricate power system challenges and teaches numerous topics as adjunct faculty. David is a patented inventor, has authored dozens of technical papers, and continues to research first principles of mission-critical technologies. Through his work, he has created methods to specify, design, and measure service level specifications for digital communication of signals, including class, source, destination, bandwidth, speed, latency, jitter, and acceptable loss. As a result, he helped coin the term operational technology (OT) to explain the difference in performance and security requirements of Ethernet for mission-critical applications versus IT applications. David is a founding member of the DNP3 Technical Committee (IEEE 1815), a founding member of UCA2, and a founding member of both IEC 61850 Technical Committee 57 and IEC 62351 for security. He is a member of IEEE, the IEEE Reliability Society, and several CIGRE working groups.

Scott Wenke received his BS degree in electrical engineering with a power emphasis from Washington State University. Prior to joining Schweitzer Engineering Laboratories, Inc. (SEL) in 2013, Scott worked at Itron. At SEL, he is a product manager in the power systems group of R&D and is responsible for transmission and substation product lines. He has been a member of IEEE since 2012.

Jaya Yellajosula received his M.Sc. and Ph.D. in electrical engineering in 2016 and 2019, respectively, from Michigan Technological University, Houghton, MI. He has worked as integration and automation engineer at Schweitzer Engineering Laboratories, Inc., since 2019. His research interests include power system protection, automation, and control in smart grids.