Security Assessment and Impact Analysis of Cyberattacks in Integrated T&D Power Systems

Ioannis Zografopoulos[*+], **Charalambos Konstantinou**[*],
Nektarios Georgios Tsoutsos[†], **Dan Zhu**[‡], **Robert Broadwater**[‡]
[*]FAMU-FSU College of Engineering, Center for Advanced Power Systems, Florida State University
[†]Department of Electrical and Computer Engineering, University of Delaware
[‡]Electrical Distribution Design
Email:{izografopoulos, ckonstantinou}@fsu.edu
tsoutsos@udel.edu, {dan.zhu, robert.broadwater}@nisc.coop

***Abstract*—In this paper, we examine the impact of cyberattacks in an integrated transmission and distribution (T&D) power grid model with distributed energy resource (DER) integration. We adopt the OCTAVE Allegro methodology to identify critical system assets, enumerate potential threats, analyze and prioritize risks for threat scenarios. Based on the analysis, attack strategies and exploitation scenarios are identified which could lead to system compromise. Specifically, we investigate the impact of data integrity attacks in inverted-based solar PV controllers, control signal blocking attacks in protective switches and breakers, and coordinated monitoring and switching time-delay attacks.**

***Index Terms*—Cyberattacks, security assessment, impact analysis, case studies, integrated power systems.**

I. Introduction

The power grid is the largest machine ever built. Electrical grids started to surface in the late 19th century providing energy to consumers, but a lot has changed since then. Nowadays, modern grid deployments enable flexible control over power generation to cover the current demand. In addition, grid modernization efforts aim to upgrade the legacy infrastructure and improve power generation and dispatch leveraging information and communication technologies (ICT) as well as renewable and distributed energy resources (DERs). DERs, being small generation or storage systems, such as rooftop solar and battery storage, apart from their much lower deployment and operation overheads, can be placed close to distribution-level consumers allowing on-site power generation and consumption, minimization of delivery costs, and increased grid resiliency due to the generation redundancy.

The increasing penetration of DERs and the ICT integration emphasizes the need for understanding the interdependency of the interactions between distribution and transmission systems. In the past, power system studies were conducted by modeling and simulating the transmission and distribution (T&D) systems independently. Recent works, however, utilize integrated T&D models demonstrating that this approach can capture grid synergies with high fidelity [1]–[3]. Fig. 1a illustrates the top level architecture of an integrated T&D system. Such models are crucial in investigating the effects of distribution systems' anomalous operation to the transmission systems, and vice versa, as well as the impact of cyberattacks holistically.

The proliferation of smart meters and smart inverters increases the threat surface and exposes the power grid to greater risk of cyberattacks [4]. Thus, threat modeling and risk assessment are important tools to identify and evaluate potential threats, as well as prioritize the corresponding risks to the power system. In this work, we employ the *OCTAVE Allegro* methodology to identify critical system assets and enumerate potential threats. We also perform a comprehensive analysis for threat scenarios and prioritize attack risks based on their expected outcomes to system operation. Moreover, our cybersecurity analysis demonstrates the impact evaluation of the identified threat scenarios. Specifically, we perform an impact analysis study for three main attack categories on an actual integrated T&D model and dataset.

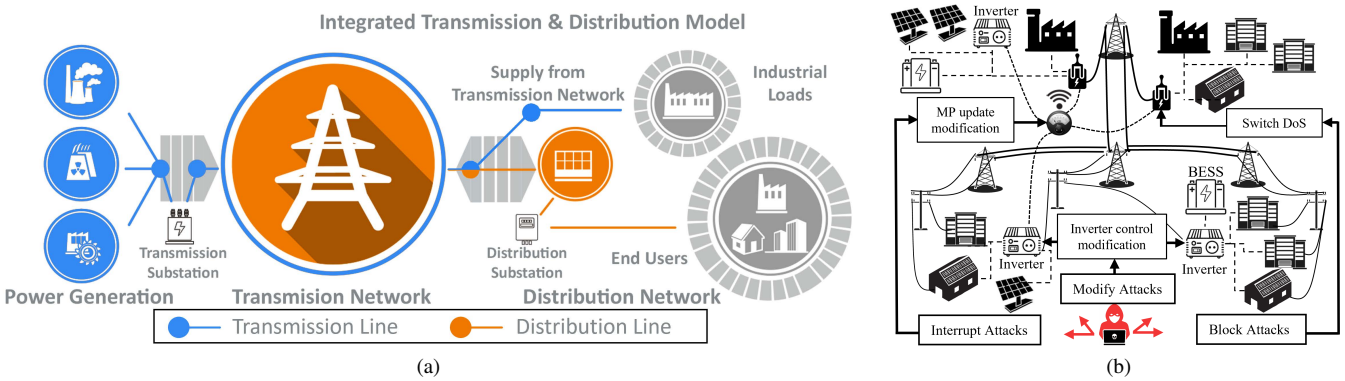
The roadmap of the paper is as follows. Section II presents the background and risk assessment method. Section III describes the attack classes, adversary objectives, and potential attack outcomes. Section IV presents the simulation setup and experimental results, while Section V concludes the paper.

II. Threat Modeling and Risk Assessment

Over the past years, power systems have experienced drastic transformations to address the growth in energy demand and enhance power quality and energy efficiency. The shift to the smart grid involves, among others, the inclusion of smart inverters, intelligent electronic devices (IEDs), and advanced metering infrastructure (AMI). Embedded device controllers are used to support communication and control functions of inverters [5]. Additionally, grid assets and their operation mechanisms (e.g., switches, breakers) are often controlled using IEDs [6]. Furthermore, AMI, such as smart meters and monitor points (MPs), enables better situational awareness and helps detect anomalous system behavior and cyberattack intrusions. The inclusion of the aforementioned components within T&D systems, however, increases the threat surface. Vulnerabilities of such units can be ported to the power grid [7], while insecure control networks and protocol implementations further exacerbate the problem [8]–[10].

We refer to mission-critical system assets that can jeopardize grid operations if compromised by malicious actors as *crown-*

[+]Corresponding author.
This work was supported in part by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technology Office (SETO) Award Number DE-EE0008768.



(a) (b)

Fig. 1. (a) Integrated transmission and distribution (T&D) model concept, (b) Power grid cyberattack scenarios.

jewels [11]. Notably, these devices include grid inverters, utility-to-device communication channels, physical interfaces, substation circuit breakers/reclosers, and controllers. Gaining access to any of these assets can enable an adversary to manipulate the generated or stored energy, cause switch disconnections altering the system topology, false trips, feeder overloadings, voltage-frequency violations, damage protection equipment, or inflict system instabilities [5], [8], [12]. In addition, the grid communication infrastructure and industrial protocols could be targeted from adversaries to mount their attacks. For example, attacks targeting DNP3 communications could exploit vendor implementation issues of the protocol, protocol specification vulnerabilities, and/or vulnerabilities in the supporting communication infrastructure. According to the Electric Power Research Institute (EPRI), more than 75% of North American electric utilities use the DNP3 protocol for industrial control applications and SCADA systems [13].

A. Security Assessment with OCTAVE Allegro

The power grid security assessment in our work is performed using the OCTAVE Allegro risk assessment methodology [14]. The first step of the analysis entails: *(i)* identification of critical system assets, *(ii)* identification of security requirements, and *(iii)* identification of security threats to the critical assets. The second step focuses on: *(i)* identifying the criteria for impact evaluation when a threat is realized, *(ii)* defining the priority/importance of the identified impact evaluation areas, and *(iii)* calculating the relative risk to each critical asset based on the probability and impact of the applicable threats. The third step defines strategies to manage the identified risks.

A threat refers to a situation or scenario in which an entity (e.g., a threat actor) or natural occurrence could cause an undesirable outcome. During the first step of OCTAVE Allegro, the security threats applicable to the critical assets are identified. Each threat is associated, and later analyzed, according to its corresponding parameters: actor, affected asset, outcome, motive, and access. Next, the threat scenarios are defined to show how a system asset is compromised if an actor, who has a motive and an access method, causes an undesired outcome to the target asset. In essence, the devised threat scenarios are useful for articulating the existing risks to critical assets.

TABLE I
CRITICAL ASSET THREAT SCENARIOS.

Affected Asset*	Outcome*	Risk Probability	Severity	Risk Score
Solar Inverters	Transient Voltage & Frequency Instability	Medium	27	54
SCADA Devices	Anomalous Grid Sectionalization & Electricity Loss	Low	31	31
Monitor Points	Loss of Situational Awareness & Erroneous Control	Medium	15	30

*Assumptions: Threat actor = attacker, motive = deliberate, and the access = via technical means (i.e., without physical access)

In our risk analysis, we focus on three core components of the grid infrastructure. We assume that the threat actor is a malicious adversary with deliberate motives to compromise the system. Specifically, we investigate scenarios involving DER and inverter control, SCADA controlled devices (e.g., switches, reclosers, breakers), and MPs (e.g., smart meters). In Table I, we demonstrate the three aforementioned critical assets alongside the respective threat scenarios, risk probabilities, severity, and comprehensive risk scores. The *Risk Probability* for each scenario is determined by the security analysis team and reflects how plausible it is for such an attack to occur based on the asset's location in the system, cyberphysical security perimeter, etc. *Risk Probability* is qualitatively assessed receiving scores Low (1), Medium (2), or High (3), while *Severity* represents the impact of the scenario to the grid operation. The impact areas are ranked based on the asset's objective within the system with scores from 1 to 5, with 5 being the most significant. The areas and their severity scores are: safety and health (5), financial (4), productivity (3), reputation (2), fines and legal penalties (1). Finally, the *Risk Score* is calculated as $Risk\ Probability \times Severity$, and it is used for comparisons between assets aiding the prioritization of those with the highest relative risks.

III. ATTACK CLASSES

Our analysis focuses on three attack directions, aligned with our threat modeling in Section II and depicted in Fig. 1b: *(i)* data modification attacks, *(ii)* loss/blocking attacks during

system-critical operations, and *(iii)* interruption of system-critical operations attacks.

The first attack category refers to tampering attacks aiming to maliciously modify system data. Data tampering includes attack scenarios in which control commands are manipulated without detection. Such attacks can be launched, for example, via communication channel corruption or exploitation of IED vulnerabilities. In the second category, the adversarial objective is to block operational commands in system-critical operations, i.e., commands from authorized entities are blocked when needed. For example, attackers could prevent access by overwhelming a resource with traffic overflowing its network bandwidth. In the third category, interruption of system-critical operations is enabled by delaying commands or data to grid components despite being issued by legitimate operators. This type of time-based attacks could undermine system operations by delaying real-time controls or measurements [15].

A. Modification of data: DER integrity attacks

DERs and supporting inverters serve as ancillary generation sources providing power to the grid. To control inverters and harness the generated power, two main categories of grid functions are implemented: *(i)* functions used by operators giving them direct control over the corresponding inverter operation, and *(ii)* autonomous functions which allow inverters to operate independently, making decisions based on their environment (e.g., power demand, generation capacity, connected loads, etc.). Our analysis covers the first type of functions which, among others, include limiting the output power of an inverter, setting active and reactive power limits, changing the power factor of the inverter, as well as controlling volt-var and watt-var operational modes.

Similar to grid operators, malicious users able to bypass the power system's security mechanisms, they can modify control commands or issue forged ones, altering the operation of inverters in order to destabilize the grid. Commands which could be of interest to malicious attackers are:
(i) Constant power factor (PF) mode: an inverter is maliciously set to operate at a constant PF, inductive or capacitive, which could potentially create voltage regulation issues, increase system losses, and reduce the electric system power quality.
(ii) Limit active power (P) mode: the amount of P injected by an inverter is maliciously controlled and limited to a setpoint, resulting in curtailing the injected P amount to the grid.
(iii) Constant reactive power (Q) mode: Similar to the P mode, an inverter can inject or absorb a constant amount of Q defined by a maliciously modified setpoint, causing undervoltage/overvoltage at points of common coupling.

B. Loss/blocking during system-critical operations: switch and breaker control attacks

Unexpected events can disrupt the steady-state operation of power systems leading to line overloads, frequency deviations, voltage instabilities, or even cascading outages. Such events can either be inadvertent, e.g., component or equipment failure, or intentional in the case of malicious attacks. To deal with the such events, immediate and protective actions should be taken. Typical countermeasures to prevent these undesirable effects and avoid a generalized system collapse involve power generation and dispatch coordination, and system reconfiguration via line and bus switching (through recloser controllers, switches, circuit breakers, etc.) which actively changes the system topology.

Attacks on switchers and breakers (e.g., by issuing malicious control commands to open/close) could trigger cascaded sequences of events. For example, if attackers gain access to a substation's ICT network, they could falsify circuit breaker control signals at a targeted IED, causing tripping of the IED-connected breakers. The result of maliciously controlled breakers could violate operational voltage limits and line overload conditions initiating cascading outage events. In essence, the end goal of such attacks is to open or close circuit breakers, change the system topology causing line overloads, and thus lead to serious problems including blackouts, brownouts, equipment failures, and uneconomical system operation.

C. Interruption of system-critical operations: coordinated monitoring and switching attacks

Protective switches and breakers are designed to handle power network faults (e.g., short-circuits) and sectionalize areas with sufficient response time to minimize fault duration, reroute power flow, and avoid any equipment damage. This involves isolating areas via tripping the breakers and eventually reclose circuits automatically. This operation attempts to preserve stability and minimize the impact to the rest of the system. Failure to open/close the switch/breaker may initiate chain reactions. In this category of attacks, we delay the control commands to the switching devices despite being issued by legitimate operators. At the same time, MPs due to their sporadic (i.e., with sampling intervals ranging 10-15 minutes) and unsynchronized measurements cannot effectively detect momentary time-delay malicious events. Consequently, grid situational awareness is compromised, monitoring routines cannot detect and promptly initiate mitigation strategies to avoid outage events, and adversaries stealthily mount their advanced persistent attacks undetected.

Preserving grid stability relies on responding timely to system changes (e.g., faults). Situational awareness is critical for detecting abnormalities, generating automated responses, and mitigating threats. MPs serve as the system's sensors aiding system observability and detecting malicious or anomalous behaviors. Maintaining stable operation relies heavily on retaining visibility of the system states at all times, since adversaries can create transient events that cannot be detected. For instance, short and intermittent malicious events cannot be detected by MPs if their duration is much smaller than the update frequency of the MP (e.g., 15 minutes).

IV. Simulation Setup and Results

Grid devices for monitoring and controlling the operation of power systems can regulate the voltage output and the generated power (P, Q) under varying steady-state or transient

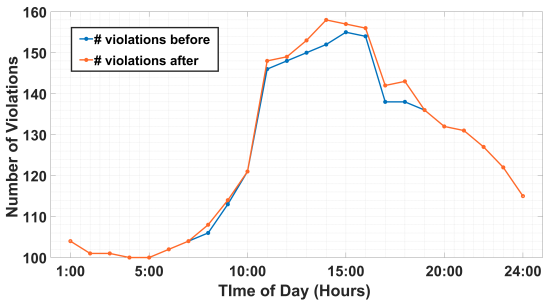


Fig. 2. Inverter violations before and after compromise.

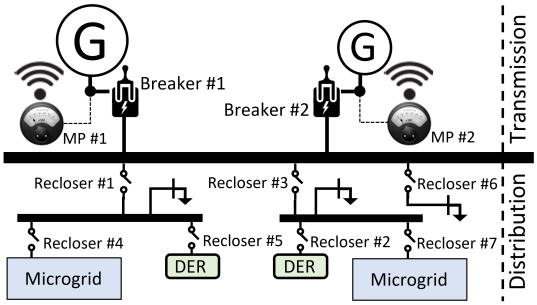


Fig. 3. Simplified integrated T&D model single line diagram.

events. As a result, such devices can control setpoints of automatic generation control functions, capacitor banks, reactors, load-tap changing transformers, and energy storage and inverter-based resources.Additionally, in many cases, network switching control is utilized by system operators to mitigate component overloading scenarios and other emergencies. The system reconfiguration, i.e., alteration of the system topology via network switching, can involve opening/closing interconnection switches using alternative T&D lines or splitting busbars to meet power demand [16]. These alternative network architectures, although they can mitigate the propagation of adverse effects, they can also lead to uneconomical operation or violation-inducing scenarios [17]. Thus, in order to evaluate the impact of the cyberattack use cases in the integrated T&D model, we utilize the number of violations as an indicator before and after the compromise.

Violation definition: With the term violation, we refer to system component behavior exceeding the nominal operational limits, and potentially compromising the stable system operation. For instance, voltage violations are triggered if the voltage at a specific system component surpasses the acceptable range, i.e., higher than $126V$ (overvoltage), or lower than $114V$ (undervoltage), for a $120V$ nominal bus voltage with a 5% allowed deviation. Similarly, we have current and power violations for components, buses, or lines, if these values exceed the prescribed limits, jeopardizing system operation, equipment performance, and human safety.

Simulation setup details: The simulation analysis and impact evaluation of the attack classes is performed using the Distributed Engineering Workstation (DEW) simulation software. Additionally, an integrated T&D model composed of 1834 T&D load points, 218 solar PV inverters, and 3,000 sectionalizing devices (e.g., cut-out switches, circuit breakers, reclosers, etc.) is employed to highlight the comprehensive impact as well as the interdependency of T&D networks.

A. Modification of data: DER integrity attacks

As discussed in Section III, DERs and inverters can support grid operation providing power either by responding to operator requests (e.g., via issued control commands) or in an autonomous fashion. In this simulation scenario, we assume that an adversary, by compromising the communication infrastructure (i.e., the communication links used by utilities to control DER assets), can modify and inject malicious commands to the deployed inverters. Specifically, the adversary maliciously controls inverters and sets them operating in a purely active (P) mode of operation, i.e., the PF is set to 1.0, while their generation limits (P, Q) have been decreased inhibiting the inverters to provide power to the grid. To illustrate the grid dependency on inverter-based generated power, we have compiled the voltage, current, and power violation reports corresponding to the aforementioned inverter control modifications. In Fig. 2, we provide a graphical representation of the generated violations throughout a day once the system's inverters get compromised. Notably, during peak working hours the number of violations is much higher, compared to early in the morning or late at night when the inverter contribution is expected to be minimal.

B. Loss/blocking during system-critical operations: switch and breaker control attacks

Fig. 3 illustrates the overall architecture of the integrated T&D system under test. We have underlined the importance of breakers and recloser switches in sectionalizing parts of the grid during adverse events impeding their spread system-wide; however, adversaries can leverage these mechanisms to compromise the system operation, leaving parts of it without power. For our analysis, we mainly focus on two sub-circuits on the distribution level since they arise as more prominent targets for adversaries compared to transmission systems which are typically better protected and monitored.

By performing power flow analysis and through maliciously modifying the behavior of SCADA controlled switches and breakers, we generate violation reports demonstrating the degree of impact introduced by such adversarial actions to the power system. The aforementioned violation reports (outlined in Fig. 4) illustrate the most critical points for the system. Hence, their security should be prioritized since they would be the most favorable targets for adversaries aiming to maximize the inflicted damage. In Fig. 4, we present the number of violations which occur in the integrated T&D system model once any of the components (on the horizontal axis) gets compromised. Furthermore, the geographic distance between the attacked device and the generation facility is indicated. We observe that there is correlation between the device proximity to the generation point and the number of violations. If a device gets compromised, all the successive devices on the

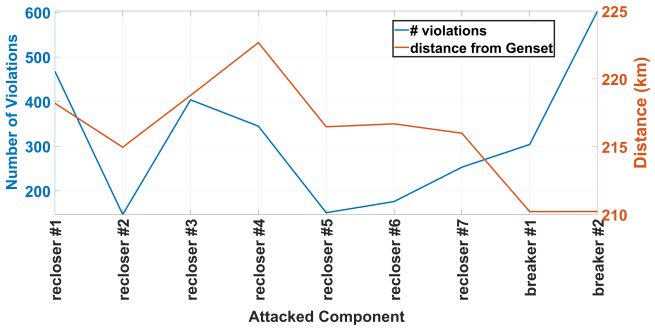


Fig. 4. Switch and circuit breaker violations.

same path will also be affected. Circuit breaker #2 arises as the most vulnerable device (also closer to the generation point), followed by reclosers #1 and #3.

C. Interruption of system-critical operations: coordinated monitoring and switching attacks

Situational awareness is essential in order to preserve power system reliability, stability, and mitigate the impact of adverse events such as blackouts and equipment failures. AMI and MPs enhance the observability of the power system states (e.g., voltage and current magnitude/angle, frequency, power, etc.) by providing regular updates to system operators. In this scenario, we consider time-delay attacks in which control commands to switches are delayed due to the lack of synchronization between system operators and MPs.

For our case study, the MPs are assumed to communicate with the control center (system operator) at regular intervals, typically in the range of 10-15 minutes, thus short transient events can pass unnoticed if properly timed between system MP sampling intervals. The knowledge of the most critical component, i.e., circuit breaker #2 per the previous attack study, can lead attackers to stealthily compromise system operation. The aforementioned device can cause 603 violations. If the attack is properly synchronized, i.e., it occurs anywhere in the 15 minute window (Fig. 5), detecting it becomes challenging. Thus, system operators can be oblivious to such severe events. Notably, the switching of the breaker is not noticed by the MP, and the reported values before switching the device remain unaltered, although we introduced a disconnect event between the MP sampling points. Similar attacks can be performed to different locations with varying system-wide impacts. In our implementation, we selected the most critical switching device, i.e., breaker #2 to emphasize the corresponding effects.

V. Conclusions

In this paper, we demonstrate how simulation-aware risk assessment analyses are critical for identifying vulnerable grid components. The security enhancement of such components could lead to more resilient power systems against cyberattacks. An integrated T&D system model is used for the attack simulations, and the OCTAVE Allegro methodology is utilized for the risk assessment process.

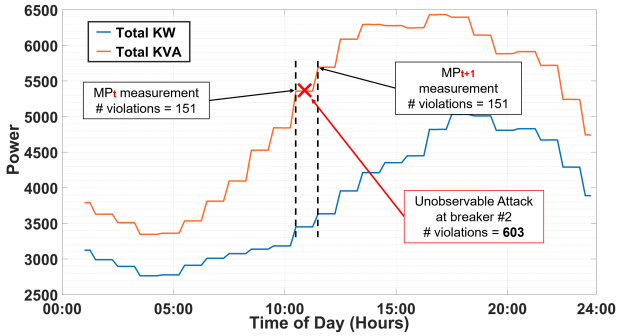


Fig. 5. Monitor point (MP) frequency update granularity.

References

[1] H. Jain, A. Parchure, R. P. Broadwater, M. Dilek, and J. Woyak, "Three-phase dynamic simulation of power systems using combined transmission and distribution system models," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4517–4524, 2016.

[2] A. Tbaileh, H. Jain, R. Broadwater, J. Cordova, R. Arghandeh, and M. Dilek, "Graph trace analysis: An object-oriented power flow, verifications and comparisons," *Electric Power Systems Research*, vol. 147, pp. 145–153, 2017.

[3] B. A. Bhatti, R. Broadwater, and M. Dilek, "Analyzing impact of distributed pv generation on integrated transmission & distribution system voltage stability—a graph trace analysis based approach," *Energies*, vol. 13, no. 17, p. 4526, 2020.

[4] A. Peedikayil Kuruvila, I. Zografopoulos, K. Basu, and C. Konstantinou, "Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids," *arXiv preprint arXiv:2009.07691*, 2020.

[5] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 28–39, 2016.

[6] C. Konstantinou and M. Maniatakos, "Impact of firmware modification attacks on power systems field devices," in *Int'l Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2015, pp. 283–288.

[7] C. Glenn, D. Sterbentz, and A. Wright, "Cyber threat and vulnerability analysis of the us electric sector," Idaho National Lab.(INL), Idaho Falls, ID (United States), Tech. Rep., 2016.

[8] J. Johnson, "Roadmap for photovoltaic cyber security," *Sandia National Laboratories*, 2017.

[9] I. Zografopoulos and C. Konstantinou, "DERauth: a battery-based authentication scheme for distributed energy resources," in *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 560–567.

[10] I. Zografopoulos, J. Ospina, and C. Konstantinou, "Special Session: Harness the Power of DERs for Secure Communications in Electric Energy Systems," in *2020 IEEE 38th International Conference on Computer Design (ICCD)*. IEEE, 2020, pp. 49–52.

[11] The MITRE Corporation, "Crown Jewels Analysis," 2019.

[12] J. Ospina, X. Liu, C. Konstantinou, and Y. Dvorkin, "On the feasibility of load-changing attacks in power systems during the covid-19 pandemic," *IEEE Access*, vol. 9, pp. 2545–2563, 2021.

[13] D. Jin, D. M. Nicol, and G. Yan, "An event buffer flooding attack in dnp3 controlled scada systems," in *Proceedings of the 2011 Winter Simulation Conference (WSC)*. IEEE, 2011, pp. 2614–2626.

[14] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies," *arXiv preprint arXiv:2101.10198*, 2021.

[15] J. Ospina, I. Zografopoulos, X. Liu, and C. Konstantinou, "Demo: Trustworthy cyberphysical energy systems: Time-delay attacks in a real-time co-simulation environment," in *Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy*, ser. CPSIOTSEC'20. New York, NY, USA: ACM, 2020, p. 69.

[16] K. W. Hedman, S. S. Oren, and R. P. O'Neill, "A review of transmission switching and network topology optimization," in *2011 IEEE power and energy society general meeting*. IEEE, 2011, pp. 1–7.

[17] N. Müller and V. Quintana, "Line and shunt switching to alleviate overloads and voltage violations in power networks," in *IEE Proceedings C – Generation, Transmission and Distribution*, vol. 136, no. 4. IET, 1989, pp. 246–253.