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

Email: {izografopoulos, cconstantinou}@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. [1] 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 on 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 the 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].
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)

We refer to mission-critical system assets that can jeopardize grid operations if compromised by malicious actors as crown-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 devices can enable an adversary to manipulate the generated or stored energy, cause switch disconnections altering the system topology, false trips, feeder overloading, 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 by 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.

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 × 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. 2: (i) data modification attacks, (ii) loss/blocking attacks during system-critical operations, and (iii) interruption of system-critical operation 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 control signals 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 are 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 overload, 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
With the term violation, we refer to the simulation analysis and im-
update frequency of the MP (e.g., 15 minutes). For instance, short and intermittent malicious events cannot be detected by MPs if their duration is much smaller than 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 are 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. 3, 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. 4 illustrates an architectural diagram of the integrated T&D system under test. It is important to note that Fig. 4 does not reflect the ‘actual’ grid interconnections and topology; for confidentiality and security reasons, the integrated T&D system model topology cannot be disclosed. Similarly, the nameplate capacities of generators, number of connected residential/commercial loads, microgrid characteristics, power

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 events. As a result, such devices can control the 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 [17]. 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.

![Inverter violations before and after compromise.](image-url)
flows, etc. are not provided since they would expose sensitive information regarding the actual power system architecture. Thus, we have sanitized the analysis results delineating critical information without open sourcing intelligence for the electric power critical infrastructure which, if maliciously exploited, could endanger the operation of the power system. Equally important to the power system topology information is the location and control of switching devices. 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 on the power system. The aforementioned violation reports (outlined in Fig. 5) 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. 5, 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 geographical 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 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.

Furthermore, although – according to Fig. 5 – breakers #1 and #2 are located at similar distances from their gensets, the number of their corresponding violations is significantly larger. This observation dictates that breaker #2 is supporting more loads (out of which some might be critical loads, thus “non-shedable”). The discrepancy between the reported violations implies that in the event of a breaker #2 trip, the loads that do not belong to DER-enabled microgrids (i.e., able to operate autonomously and meet the power demand) will have to be supported from neighbouring resources. Altering power dispatch to accommodate for such unexpected power demand leads to uneconomical grid operation, and hence, more violations. For our case study, the number of violations serves as an “performance indicator”. In other words, more violations outline worse grid operation conditions.

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 operation and MPs.

For our case study, the MPs are assumed to communicate with the control center (system operator side) 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 the 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. 6), 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 on 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.

Security Discussion: The goal of our analysis is to demonstrate that simulation-aided risk assessment is a useful tool
for evaluating the condition of system operations. The proposed framework can be employed to identify power system related vulnerabilities, examine the efficiency of mitigation strategies against such vulnerabilities, and design redundancy measures to overcome cyberattacks or unexpected failures. Our methodology serves as a proof-of-concept in this direction, and as such, the violation terminology can assume different definitions depending on the type of analysis being conducted and the nature of the system being investigated. For example, if we are simulating an attack scenario on switch and breaker controls, the number of violations could indicate the number of compromised/offline devices, loads being shed, overloaded lines, sectionalized power equipment, etc. On the other hand, if we are conducting a data integrity or injection attack type of study where adversaries aim to falsify the locational marginal price (LMP) mechanism, violations could be triggered if the electricity price surpasses a certain threshold yielding uneconomical grid operation. Regardless of the case study and the investigation-specific characteristics, the synergetic application of system simulations and risk assessment is beneficial in designing secure and resilient power systems.

V. CONCLUSIONS

In this paper, we present a cybersecurity analysis encompassing risk and impact assessment of power grids with DERs. Three different attack classes are discussed including data integrity attacks, alongside attacks aiming to block and interrupt critical grid functions. Furthermore, 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 impact evaluations, while the OCTAVE Allegro methodology is utilized for the risk assessment process.

DISCLAIMER

This paper was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

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. Arghande, 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, 2017.

[6] C. Konstantinou and M. Maniatakis, “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. 356–367.

[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,” 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,” IEEE Access, vol. 9, pp. 1–44, 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 IEEE Proceedings C – Generation, Transmission and Distribution, vol. 136, no. 4. IET, 1989, pp. 246–253.