Impact Assessment of Cyberattacks in Inverter-Based Microgrids

Kerd Topallaj, Colin McKerrell, Suraj Ramanathan, Ioannis Zografopoulos
Engineering Department
University of Massachusetts Boston
Boston, MA, USA
{kerd.topallaj001, colin.mckerrell001, suraj.ramanathan001, i.zografopoulos}@umb.edu

***Abstract*—In recent years, the evolution of modern power grids has been driven by the growing integration of remotely controlled grid assets. Although Distributed Energy Resources (DERs) and Inverter-Based Resources (IBR) enhance operational efficiency, they also introduce cybersecurity risks. The remote accessibility of such critical grid components creates entry points for attacks that adversaries could exploit, posing threats to the stability of the system. To evaluate the resilience of energy systems under such threats, this study employs real-time simulation and a modified version of the IEEE 39-bus system that incorporates a Microgrid (MG) with solar-based IBR. The study assesses the impact of remote attacks impacting the MG stability under different levels of IBR penetrations through Hardware-in-the-Loop (HIL) simulations. Namely, we analyze voltage, current, and frequency profiles before, during, and after cyberattack-induced disruptions. The results demonstrate that real-time HIL testing is a practical approach to uncover potential risks and develop robust mitigation strategies for resilient MG operations.**

***Index Terms*—Cyberattack, hardware-in-the-loop, microgrid, real-time simulation.**

I. Introduction

The growing penetration of Distributed Energy Resources (DERs) – such as photovoltaic (PV) arrays, wind turbines, and energy storage systems – requires new approaches to maintain grid reliability and stability. The Microgrid (MG) concept has emerged as a key solution for integrating and managing both renewable and non-renewable DERs [1]. According to the National Renewable Energy Lab (NREL) definition, a MG is "*a group of interconnected loads and DERs that acts as a single controllable entity with respect to the grid*" [2]. Furthermore, MGs can operate in both grid-connected and islanded modes, exchanging power with the main grid or operating autonomously to support local loads.

This flexibility makes MGs essential components for maintaining power system stability during grid disturbances resulting from accidental events, e.g., faults, or malicious incidents, e.g., cyberattacks. A MG's ability to coordinate generation and demand at the local level enhances resiliency, reduces operational costs, and can defer transmission and distribution network expansion plans. Furthermore, MGs offer System Operators (SO) the flexibility to respond to rapid fluctuations in on-site demand and supply by supporting high shares of Inverter-Based Resources (IBR) and enabling decentralized control.

As the integration of DERs and MGs continues to grow, ensuring their secure and resilient operation under both normal and disruptive conditions becomes increasingly critical. One of the primary areas of interest involves assessing the performance of MG under adverse conditions, such as cyberattacks or unintentional faults, and examining their potential to trigger forced islanding events [3]. These islanding transitions sectionalize MGs from the main grid at their Point of Common Coupling (PCC), which is typically controlled by a Circuit Breaker (CB). Rapid shifts between grid-connected and islanded modes can induce transient instability, frequency deviations, and voltage fluctuations, potentially compromising system reliability [4]. Traditional testing methods focusing on offline simulations are often unable to capture real-time dynamic phenomena, while experimenting on the actual power systems or even smaller deployments is cost-prohibitive and could raise safety issues. As a result, it is essential to experiment with high-fidelity system models that respect the mission-critical and time-sensitive nature of the power system's critical infrastructure, without impacting actual grid operations [5].

Recent advances in real-time Hardware-in-the-Loop (HIL) simulation offer a powerful solution to assess MG behavior before field deployment. By integrating power system models with external hardware, HIL enables realistic testing of operational stability and cyber-threats in a controlled environment, i.e., the cyber-physical testbed. Unlike purely software-based simulations, HIL provides real-time feedback by allowing interaction with physical controllers, inverters, and protection devices. Additionally, HIL methods reduce operational risks and enhance grid security by detecting vulnerabilities before real-world implementation.

The contributions of this work are the following:

- We combine essential power system assets and a MG into an integrated Transmission and Distribution (TnD) model. For the transmission-level system we use the IEEE 39-bus system, while the MG is comprised of a PV farm complemented by synchronous generation.
- We study the impact of sophisticated cyberattacks that, after identifying an anomalous grid condition, e.g., fault, they rapidly toggle the CB at the PCC, switching the MG between islanded and grid-connected modes, and stressing the MG's capacity to maintain stability.
- We present real-time simulation results to illustrate the impact of different IBR penetration levels on nominal operations and their potential to exacerbate grid instability.

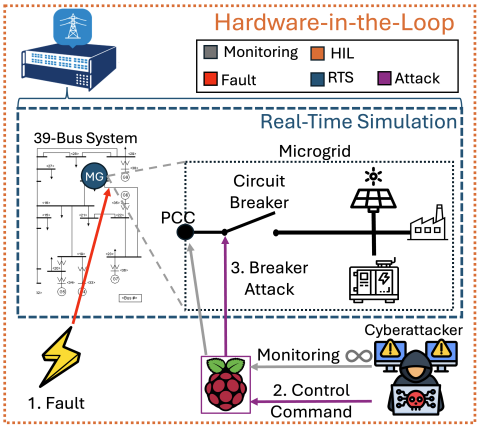

Fig. 1. System overview and attack methodology.

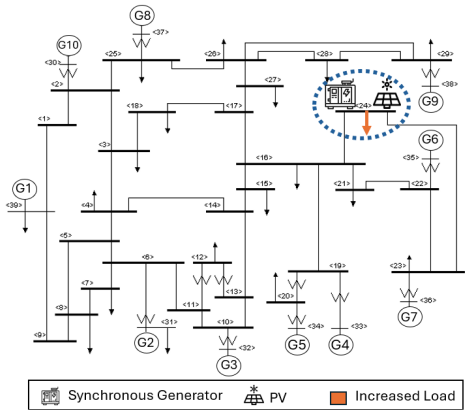

Fig. 2. Modified IEEE 39-bus transmission system.

An overview of the developed TnD system and the cyberattack kill chain is shown in Fig. 1. The remainder of this paper is organized as follows. Section II outlines the methodology, including the MG system model and the implementation of cyberattack scenarios. Section III presents the simulation configuration and results under various attack conditions and generation mixes, analyzing their impact on system stability, frequency response, and voltage waveforms. Finally, Section IV concludes the paper and discusses directions for future work.

II. Methodology

The following subsections detail the power system model and the modifications performed to the IEEE 39-bus system to integrate the inverter-based MG. We also outline the adversary model and cyberattack assumptions adopted in this study.

A. System Model

This study uses the IEEE 39-bus transmission system to evaluate the performance and stability of an autonomous MG. As shown in Fig. 2, the system comprises 10 synchronous generators, 34 transmission lines, 12 transformers, and 19 aggregated loads [6]. The original New England system includes only synchronous generators. However, inverter-based DERs (specifically a PV farm), which lack natural inertia are integrated alongside conventional sources to reflect evolving generation portfolios. Different PV penetration levels are examined in Section III to assess their impacts on system stability.

To reflect the MG's behavior in real-time during islanded operation, the PV inverter is configured to operate in a Grid-Forming (GFM) fashion. GFM inverters can independently regulate voltage and generate their own frequency reference, making them suitable for autonomous operation. Furthermore, bus 24 is selected as the MG interconnection point, as shown in Fig. 2 (blue circle). The additions of PV penetration and a synchronous generator are also connected to bus 24. Although bus 24 is not directly connected to any generator, it is electrically adjacent to bus 23 and G7. This location could become a prominent target for an attacker aiming to propagate impacts to adjacent generators and loads.

To evaluate the impact of adverse events on a stressed operational scenario, the load demand at bus 24 is increased by 20%, indicated by the orange arrow at the bus in Fig. 2. This could represent residential or industrial load excursions during abnormal conditions, enabling the evaluation of weakly-connected MG performance under high-loading conditions. Additionally, a single-phase-to-ground fault is introduced at bus 24 to assess the MG's ability to sustain the local loads during fault conditions. Without localized generation, such faults can lead to instability. However, with the MG in place, the grid's post-fault dynamic behavior should be analyzed.

B. Adversary Model

The adversary model defines the attacker's capabilities, knowledge, and access [7]. In this work, the adversary is assumed to have partial system knowledge, specifically, awareness of the remotely accessible communication interface of the CB. This reflects a gray-box threat model in which the attacker lacks complete visibility into the bulk power system but understands how to launch targeted attacks against the MG.

The adversary can remotely access and control a Raspberry Pi used as the cyber interface to the CB that connects the MG with the rest of the system, as seen in Fig. 1. This device enables remote attacks, such as timed CB switching attacks, delivered during vulnerable conditions, e.g., grid faults or peak loading. The attacker aims to destabilize the MG by forcing repeated transitions between grid-connected and islanded modes, potentially causing cascading failures and blackouts. By timely coordinating their attack, the risk for grid destabilization could increase during abnormal events. Thus, the adversary aims to leverage such a condition, i.e., during a single-phase-to-ground fault at bus 24, to maximize their impact on the system.

The attacker could be classified as a Class I adversary, as defined in [7]. While they possess moderate resources and remote access to the CB, their ability to carry out the attack covertly is limited. Although a single unauthorized transition may not trigger system-wide consequences, repeated and intentional switching at the MG's PCC would likely be flagged by system operators as suspicious activity.

C. Attack Methodology

The attack model describes how a system vulnerability could be exploited to become a system-level threat [8]. In our case, the attacker targets the CB at the MG PCC, aiming to trigger unintentional islanding conditions. The primary vulnerabilities of the MG lie in the insecure communication interfaces used by SO to issue grid islanding commands by tripping the CB at the PCC [4], [8]. Furthermore, sophisticated attackers can leverage the increased reliance of MGs on predominantly IBR-based generation to maximize their attack impacts since, unlike synchronous generators, IBR resources lack inertia, making them unable to "absorb" sudden disturbances. Thus, the CB becomes a high-impact target given its remote accessibility and limited built-in security. Once it is compromised and maliciously operated, it can jeopardize system stability, as we demonstrate in Section III [9].

To exploit the identified vulnerabilities, the attack is carried out using a Raspberry Pi, which transmits unauthorized actuation signals to the CB, modeled in the OPAL-RT real-time simulation environment. The attack orchestration, shown in Fig. 1, includes the following stages. Under normal system conditions, the attacker employs the Raspberry Pi to passively monitor critical grid parameters, such as voltage and frequency, without initiating any active interference. This phase aims to collect system measurements and establish a baseline understanding of the grid's behavior. The attack is initiated once the adversary identifies an abnormal operating condition, such as a fault. The detection of abnormal grid conditions, achieved by closely analyzing the grid's real-time measurements, serves as the trigger for the attack.

Once an abnormal scenario is detected, the attacker orchestrates the attack. This involves overriding the legitimate control logic of the system by issuing malicious commands to the CB (either to open or close it), thereby disrupting the grid's functionality [10]. The attacker can manipulate the CB to isolate a portion of the grid through a single actuation, commonly referred to as a forced islanding attack (*Scenario 1* in Table I). Alternatively, the attacker may repeatedly issue commands to connect/disconnect the CB multiple times, creating a switching attack (*Scenario 2*). Following these steps, the attacker aims to disrupt the power grid, causing potential operational and reliability consequences.

III. Simulation Results

The following subsections delineate the experimental setup and outline the various simulation scenarios analyzed to evaluate the impact of cyberattack-induced islanding.

A. Experimental Setup

For our experiments, we utilize the IEEE-39 bus model, which has been modified to incorporate a MG (Fig. 2). The integrated TnD model is developed using MATLAB Simulink and Simscape Electrical on a Windows-based workstation. This TnD model is deployed onto the real-time simulator (OPAL-RT OP4610XG) to enable time-synchronized execution and interaction between the real-time environment and the external control node (Raspberry Pi 4) which has been maliciously compromised.

TABLE I
Cyberattack Test Cases Information

MG Generation	**Scenario 1**	**Scenario 2**
System I: 150MW PV & 150MW Synchronous	Islanding at $t = 1$s, reconnection at $t = 1.5$s	CB switching (6 times) between $t = 1$s and 1.5s
System II: 210MW PV & 90MW Synchronous		

An overview of the experimental setup is illustrated in Fig. 1, where the Raspberry Pi is configured as an external, remotely accessible cyberattack vector. Communication between the real-time simulator and the Raspberry Pi is established using User Datagram Protocol (UDP). This network configuration enables the transmission of real-time data and control signals between the two devices.

B. Cyberattack Test Cases

In Table I we summarize the specifics of the four different simulation test cases used in this work. In *System I*, the 300 MW of power generated in the MG is evenly distributed (50% – 50% split) between PV and synchronous generation, while in *System II*, the MG operates with 70% PV generation (210 MW) and 30% synchronous generation (90 MW). Each of the aforementioned test systems is then examined under two distinct scenarios. In *Scenario 1* (*single forced islanding*), the attacker issues two commands: the first trips the CB at the PCC, isolating the MG from the main grid, and the second recloses the CB, restoring grid connection. In *Scenario 2* (*CB switching attack*), the attacker rapidly toggles the CB, causing the MG to oscillate between islanded and grid-connected modes for three consecutive times.

1) System I – Balanced IBR and Synchronous MG Generation: The following scenarios evaluate the stability of the MG with balanced PV and synchronous generation.

a) Single Forced Islanding Scenario: The attacker trips the CB once to island the MG. Fig. 3 shows the frequency response at the MG at bus 24. According to the IEEE 1547 standard, the frequency should remain between the over-frequency threshold (OF1) of 61 Hz and the under-frequency threshold (UF1) of 58.5 Hz [11].

At $t \approx 1$ s, when the CB opens, the frequency dips slightly and exhibits small oscillations below 60 Hz. These oscillations remain limited, indicating that local generation stabilizes quickly in islanded mode. At $t \approx 1.5$ s, reconnection causes a transient spike (60.08 Hz) followed by a dip below 59.96 Hz before settling near the nominal frequency. This larger deviation reflects the challenge of synchronizing two previously decoupled systems, i.e., the main grid and MG. Overall, reconnection induces greater frequency swings than disconnection, but the MG stabilizes within one second. Although the islanded frequency remains within 0.04 Hz of the nominal range, some frequency excursions still exist as a byproduct of the reduced inertia within the MG as the synchronous generator only supports half of the MG's load demand.

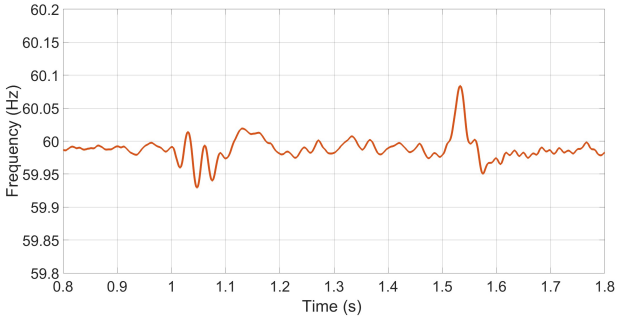

Fig. 3. Frequency response at the MG (Bus 24) during forced islanding at $t = 1\,\text{s}$ and reconnection at $t = 1.5\,\text{s}$.

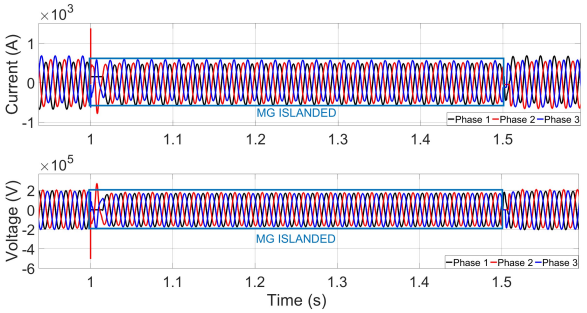

Fig. 4. Voltage and current waveforms at the MG (Bus 24) during forced islanding at $t = 1\,\text{s}$ and reconnection at $t = 1.5\,\text{s}$.

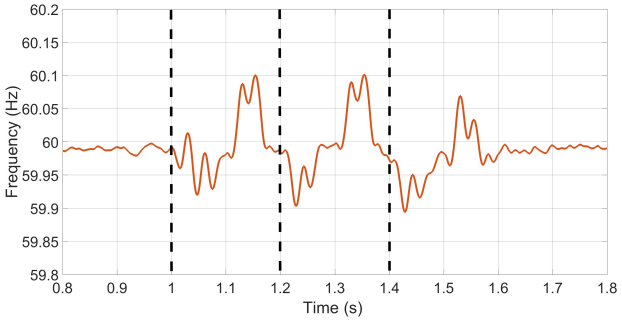

Fig. 5. Frequency response at the MG (Bus 24) during switching attacks happening at $0.1\,\text{s}$ intervals from $t = 1\,\text{s}$ to $t = 1.5\,\text{s}$.

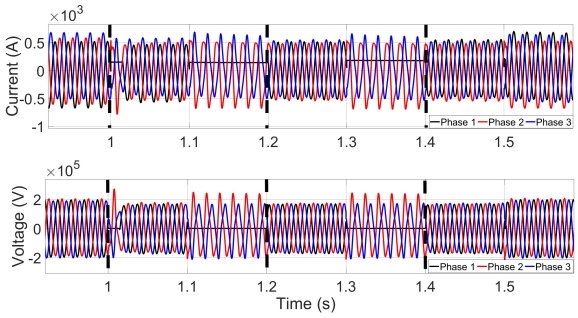

Fig. 6. Voltage and current waveforms at the MG (Bus 24) during switching attacks happening at $0.1\,\text{s}$ intervals from $t = 1\,\text{s}$ to $t = 1.5\,\text{s}$.

Fig. 4 shows the voltage and current waveforms at the MG at bus 24. Upon islanding, both quantities decrease slightly in amplitude, but remain sinusoidal and stable, indicating successful local power delivery. Upon reconnection, they return to nominal levels after a brief transient spike, demonstrating fast synchronization with minimal disruptions.

b) CB Switching Attack Scenario: In this case, the attacker switches the CB on and off three times. Fig. 5 presents the frequency response at the MG. The CB is opened every 0.2 seconds between $t = 1.0\,\text{s}$ and $t = 1.5\,\text{s}$ and is closed 0.1 seconds after each opening. In Fig. 5, the dashed black lines indicate CB openings. Each CB opening results in a sharp frequency drop, and since the CB closes before full recovery, the effects compound with each attack cycle. Subsequent islanding events deepen the frequency dips, threatening MG stability, and upon each reconnection, the frequency briefly spikes to around 60.1 Hz. Lastly, during the final reconnection at $t = 1.5\,\text{s}$, the frequency spike is approximately 0.04 Hz lower than earlier events, suggesting that the synchronous generation of the main system provides most of the inertia required to attenuate repeated disturbances.

Fig. 6 shows the three-phase voltage and current waveforms at bus 24 during this attack. Vertical dashed lines denote islanding transitions that begin at $t = 1\,\text{s}$, with rapid cycling until the final reconnection at $t = 1.5\,\text{s}$. In islanded mode, voltage and current remain sinusoidal across all phases, though with reduced magnitudes. Upon grid reconnection, Phase 1 voltage and current drop to zero due to a fault, redirecting power flow to ground. Phases 2 and 3 compensate with increased peak currents to account for Phase 1. Phase voltage asymmetries could potentially lead to overloading, thereby increasing system losses and reducing reliability. Prolonged operation under such imbalances can cause excessive heating, accelerate equipment degradation, and raise the likelihood of premature failure of grid components and insulation.

2) System II – IBR-dominated MG Generation: The following scenarios examine the stability of the MG with a 70% IBR and 30% synchronous generation mix.

a) Single Forced Islanding Scenario: In this scenario, the attacker switches the CB twice: once to island the system at $t = 1\,\text{s}$, and once to reconnect it at $t = 1.5\,\text{s}$. Fig. 7 shows the frequency response measured at the MG at bus 24 during these two key events. Following islanding, the frequency exhibits a more pronounced dip compared to *System I* due to the reduced contribution of synchronous generation. While the frequency remains within acceptable limits, the lower system inertia makes it more vulnerable to sudden disturbances. Between $t = 1\,\text{s}$ and $t = 1.5\,\text{s}$, the frequency oscillates around 60 Hz, similar to *System I*, with no significant degradation in stability. After reconnection at $t = 1.5\,\text{s}$, the initial frequency spike is comparable to that in *System I*, but the system takes slightly longer to stabilize in the grid-connected state. Nonetheless, the frequency settles near 60 Hz within approximately one second, confirming that the MG maintains sufficient control capability even with reduced synchronous support.

b) CB Switching Attack Scenario: The attacker triggers the CB three times within a 0.5-second window. The CB is opened every 0.2 seconds between $t = 1.0\,\text{s}$ and $t = 1.5\,\text{s}$ and is re-closed 0.1 seconds later each time. Fig. 8 shows the resulting frequency response. Each CB opening causes a

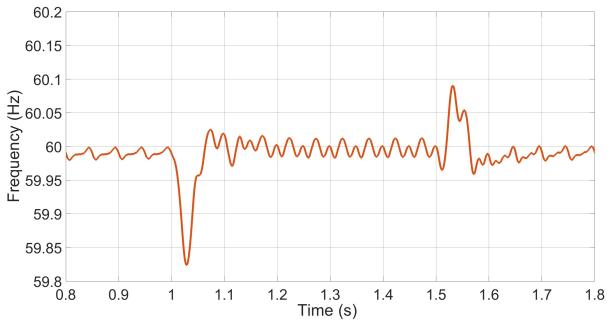

Fig. 7. Frequency response at the MG (Bus 24) during forced islanding at $t = 1\,\text{s}$ and reconnection at $t = 1.5\,\text{s}$.

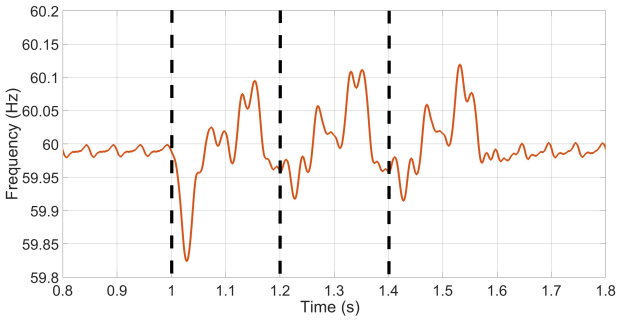

Fig. 8. Frequency response at the MG (Bus 24) during switching attacks happening at $0.1\,\text{s}$ intervals from $t = 1\,\text{s}$ to $t = 1.5\,\text{s}$.

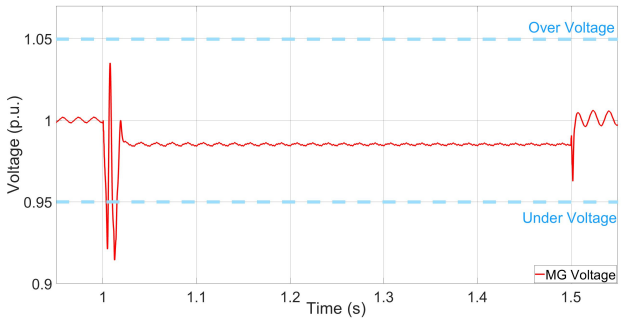

Fig. 9. Voltage magnitude p.u. at the MG (Bus 24) during forced islanding at $t = 1\,\text{s}$ and reconnection at $t = 1.5\,\text{s}$.

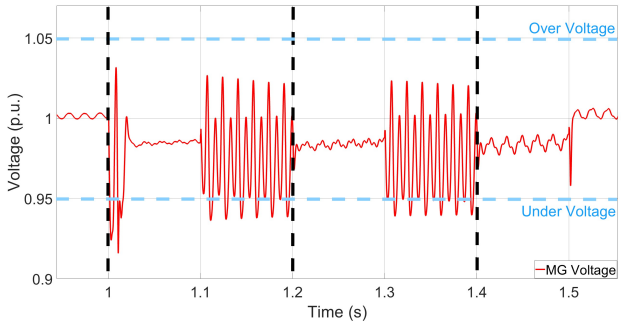

Fig. 10. Voltage magnitude p.u. at the MG (Bus 24) during switching attacks happening at $0.1\,\text{s}$ intervals from $t = 1\,\text{s}$ to $t = 1.5\,\text{s}$.

sharp frequency dip followed by a spike upon reconnection. However, the reduced inertia from the lower synchronous generation results in more pronounced frequency deviations. The first islanding event at $t = 1\,\text{s}$ causes the frequency to dip below 59.85 Hz. Unlike *System I*, the frequency during islanded intervals does not become progressively more stable with each successive event. Instead, the frequency spikes upon reconnection become increasingly pronounced, reaching nearly 60.15 Hz after the final reconnection. Despite these variations, the frequency remains within the prescribed OF1 and UF1 bounds of [11] throughout the attack sequence and shows no signs of critical instability before or after these events.

C. Voltage Stability of MG During Islanding

Fig. 9, 10, 11, and 12 illustrate the MG voltages in both scenarios for each of the two systems described in Table I. As discussed in [12], the typical MG voltage limits of 0.95 and 1.05 p.u. are denoted in each Fig. using blue dotted lines.

Fig. 9 illustrates the MG voltage in *System I, Scenario 1*. At the moment of forced islanding (1 second), the voltage drops below 1 p.u. and then rebounds above 1 p.u. MG voltage exceeds the undervoltage limits of 0.95 p.u. at the moment of islanding, indicating potential transient instability due to the fault existing in the system. For the duration of the islanding, the voltage remains within nominal values, indicating a stable MG. Upon reconnection (1.5 seconds), there is a transient dip, followed by stabilization to 0.97 p.u. within 0.01 seconds.

Fig. 10 illustrates the MG voltage in *System I, Scenario 2*. At the moment of the first forced islanding (1 second), the voltage dips and rebounds similarly to Fig. 9. During forced grid connection, seen after the vertical dashed lines, the MG voltage experiences instability, oscillating around 1 p.u. After the first islanded condition, the following islanded conditions show no transient spikes and resemble the nominal grid-connected conditions, showcasing a stable islanded MG. However, at the moments of reconnection (i.e., 1.1 seconds) the voltage momentarily drops below the 0.95 p.u. limit, causing instability in the MG, as it is forced to reconnect. The final grid connection (1.5 seconds) occurs as the fault clears and the MG voltage returns to nominal operation.

Fig. 11 illustrates the MG voltage in *System II, Scenario 1*. At the moment of forced islanding (1 second), the voltage drops below 1 p.u. and then rebounds above 1 p.u. (similar to Fig. 9). However, the oscillations in Fig. 11 are retained for almost double the duration (as opposed to Fig. 9) and exhibit higher voltage drops. Furthermore, the MG voltage appears noisier, which is mainly attributed to the inverter's inability to regulate the voltage level. Following the transient spikes, the voltage stabilizes, and upon reconnection at 1.5 seconds, the voltage is brought to 0.97 p.u. within 0.06 seconds. Overall, this indicates a stable MG despite the attack; however, in this scenario, the duration and amplitude of the transient spikes are increased with increased IBR generation.

Finally, Fig. 12 illustrates the MG voltage in *System II, Scenario 2*. At the moment of the first forced islanding (1 second), the voltage dips and rebounds similarly to Fig. 10, except with prolonged and more severe magnitude transients. However, the transient spikes during grid-connected attacking conditions are more severe, as shown by increased peak and trough magnitudes. Additionally, during MG islanding, the voltage operates below 1 p.u. for a prolonged duration and exhibits

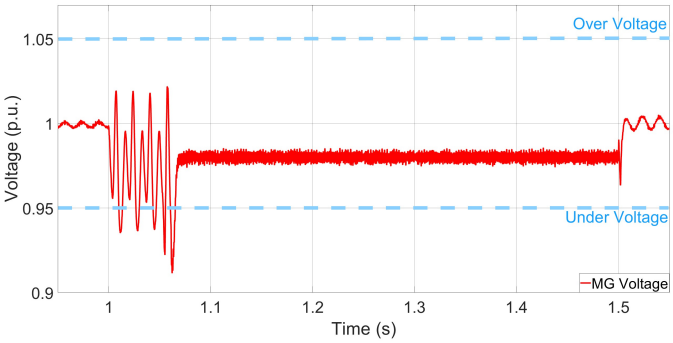

Fig. 11. Voltage magnitude p.u. at the MG (Bus 24) during forced islanding at $t = 1\,\text{s}$ and reconnection at $t = 1.5\,\text{s}$.

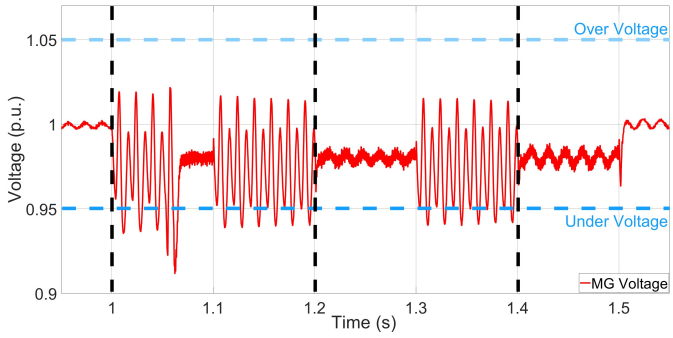

Fig. 12. Voltage magnitude p.u. at the MG (Bus 24) during switching attacks happening at 0.1 s intervals from $t = 1\,\text{s}$ to $t = 1.5\,\text{s}$.

TABLE II
SUMMARY OF SYSTEM RESPONSES UNDER CYBERATTACK SCENARIOS

Test Case	Frequency	Voltage	Key Observations
System I, Scenario 1	Minor dips during switching, fast recovery	Stable	Minimal disruption during islanding and reconnection
System I, Scenario 2	Oscillations with deeper troughs during switching	Slight UV	Switching causes compounding instability
System II, Scenario 1	Larger transients	Longer time to stabilize	More PV increases frequency/voltage disturbances
System II, Scenario 2	Deep oscillations	Severe UV	Most unstable case with high-risk of phase imbalance

lower values than in Fig. 10. Furthermore, the MG voltage exceeds the Undervoltage (UV) limits during reconnection.

Table II summarizes the frequency and voltage responses for each test case. As the table shows, PV penetration levels and number of CB switches make the system more vulnerable to disturbances. Overall, the results confirm that the MG voltage stays within acceptable operational limits across all test scenarios during islanding, demonstrating stable behavior during both single and multiple forced islanding events. However, the MG operates below the threshold voltage limits when it is forced to reconnect, causing significant voltage spikes across all voltage phases. At the same time, the transition from a balanced 50%–50% generation split to a 70% IBR-based MG furnishes more severe transient spikes and longer stabilization times when the MG transitions between islanded and grid-connected modes. The results highlight that increasing IBR penetration inherently heightens the MG's susceptibility to abrupt disturbances due to lack of inertia. Such observations could be exploited by threat actors aiming to maximize their attack impact, leveraging improperly secured grid devices (in our case the CB) to mount their attacks.

IV. CONCLUSION

This paper investigates the behavior of an integrated TnD system under coordinated switching attacks, leading to MG islanding. The developed TnD system model couples the IEEE 39-bus transmission network with an MG at the distribution level, which uses a mix of IBR and synchronous generation. We present real-time measurements, e.g., voltage, current, and frequency, during different attack scenarios demonstrating the effects that different IBR penetration levels can induce on MG behavior. Future work will incorporate additional IBR resources such as Battery Energy Storage System (BESS) and increasing PV penetrations as well as additional attack scenarios, highlighting the impact on stability of increased IBR penetration during adverse events.

REFERENCES

[1] D. Espín-Sarzosa *et al.*, "Microgrid Modeling for Stability Analysis," *IEEE Transactions on Smart Grid*, vol. 15, no. 3, pp. 2459–2479, 2024. [Online]. Available: https://doi.org/10.1109/TSG.2023.3326063

[2] National Renewable Energy Laboratory (NREL), "Microgrids," 2024. [Online]. Available: https://www.nrel.gov/grid/microgrids.html

[3] I. Zografopoulos and C. Konstantinou, "Event-triggered islanding in inverter-based grids," *Electric Power Systems Research*, vol. 243, p. 111472, 2025.

[4] I. Zografopoulos *et al.*, "Security assessment and impact analysis of cyberattacks in integrated T&D power systems," in *Proc. of the 9th workshop on modeling and simulation of cyber-physical energy systems*, 2021, pp. 1–7.

[5] K. Katuri, I. Zografopoulos, H. T. Nguyen, and C. Konstantinou, "Experimental impact analysis of cyberattacks in power systems using digital real-time testbeds," in *2023 IEEE Belgrade PowerTech*. IEEE, 2023, pp. 1–6.

[6] P. Demetriou, J. Quirós-Tortós, and E. Kyriakides, "When to Island for Blackout Prevention," *IEEE Systems Journal*, vol. 13, no. 3, pp. 3326–3336, 2019.

[7] 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. 29 775–29 818, 2021.

[8] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations," *IEEE Systems Journal*, vol. 17, no. 4, pp. 6695–6709, 2023.

[9] P. Kertzner, C. Carter, and A. Hahn, "Crown jewels analysis (cja) for industrial control systems (ics)," MITRE, Tech. Rep. PR-22-2824, December 2022. [Online]. Available: https://www.mitre.org/sites/default/files/2023-01/PR-22-2824-Crown-Jewels-for-Industrial-Control-Systems.pdf

[10] MITRE ATT&CK for ICS, "Unauthorized Command Message," 2025, accessed: 2025-03-19. [Online]. Available: https://attack.mitre.org/techniques/T0855/

[11] "IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003)*, pp. 1–138, 2018.

[12] H. Gan, J. Wang, Y. Lin, S. Bhela, and C. Bilby, "Performance Evaluation of Peer-to-Peer Distributed Microgrids Coordination for Voltage Regulation," in *2022 IEEE Power & Energy Society General Meeting (PESGM)*, 2022, pp. 1–5.