IEEE Open Access Journal of Power and Energy

Received 24 February 2025; revised 14 June 2025; accepted 26 July 2025.
Date of publication 4 August 2025; date of current version 8 August 2025.

Digital Object Identifier 10.1109/OAJPE.2025.3595631

MaDIoT 3.0: Assessment of Attacks to Distributed Energy Resources and Demand in a Power System

NÉSTOR RODRÍGUEZ-PÉREZ[1], JAVIER MATANZA[1], LUKAS SIGRIST[1] (Member, IEEE), JOSÉ RUEDA TORRES[2] (Senior Member, IEEE), AND GREGORIO LÓPEZ[1]

[1]Institute for Research in Technology, Comillas Pontifical University, 28015 Madrid, Spain
[2]Faculty of EEMCS, Delft University of Technology, 2628 CD Delft, The Netherlands

CORRESPONDING AUTHOR: N. RODRÍGUEZ-PÉREZ (nestor.rodriguez@iit.comillas.edu)

This work was supported in part by European Union's Horizon Europe Research and Innovation Program through the eFORT Project under Grant Agreement 101075665 and in part by the European Union's Horizon 2020 Research and Innovation Program through the Integrated Solutions for Positive Energy and Resilient Cities (RESPONSE) Project under Grant Agreement 957751.

ABSTRACT The increasing penetration of Distributed Energy Resources (DER) expands the cyberattack surface of power systems. This paper analyses, using PowerFactory, the impact and success of MaDIoT 3.0 attacks in the PST-16 model, a simplified model of the European system. MaDIoT 3.0 attacks are a novel type of attack that manage to compromise both high-wattage IoT demand devices and DER devices at the same time. The results indicate that the inclusion of distributed solar PV generation in the PST-16 system reduces the success ratio and impact of load-altering MaDIoT attacks when compared to the same system without DER, mainly due to an increment of the initial voltages. For MaDIoT 3.0 attacks, the demand had a more significant influence on the attack's success than DER in the PST-16 system. Distributing the attacked demand across more buses or targeting the demand from other areas would decrease the success ratio of the attack. Therefore, the local scalability and replicability of vulnerable high-wattage demand devices in the analysed system become more critical than their distributed deployment in larger areas.

INDEX TERMS Cyberattack, power system dynamics, MaDIoT, load altering attacks, distributed energy resources, power system stability.

I. INTRODUCTION

THE issue of cybersecurity in power systems has gained attention in recent years. With the increasing deployment of Internet of Things (IoT) devices and Distributed Energy Resources (DER), cyberattacks are not limited to just utilities' Supervisory Control And Data Acquisition (SCADA) systems. Instead, attackers may also take advantage of the weaknesses present in these devices. Furthermore, the monitoring of high-wattage devices such as electric vehicle charging points may not be consistently conducted by the System Operator (SO) [1].

Cyberattacks that manipulate demand—such as load-altering attacks [2], [3] and MaDIoT (Manipulation of Demand via IoT) attacks [4]—can disrupt grid stability by triggering load shedding or generator protection mechanisms [5], [6], [7], [8], [9], [10], or by distorting energy markets [11]. However, the success and impact of these attacks are highly dependent on the characteristics of the power system under attack [12], [13].

In parallel, DERs—such as solar PV installations—are increasingly integrated into distribution networks and are also vulnerable to cyberattacks. These attacks can target DER communications [14] or devices themselves [15], potentially causing voltage regulation issues [16], transient frequency instability [17], [18], or even forced disconnections through compromised inverters or abnormal voltage conditions induced [19]. In particular, Bräunlein and Melette demonstrated at the 38th Chaos Communication Congress that the unencrypted radio signals used by DERs can be exploited to compromise renewable energy facilities [20]. Technologies such as Radio Ripple Control, widely used in central Europe [21], [22], are particularly susceptible.

Despite the growing research on attacks targeting demand or DERs, no prior research has analysed the potential impact

of combined cyberattacks on both demand-side IoT devices and DERs. This constitutes a research gap, especially as smart grid technologies increasingly integrate these components through Energy Management Systems (EMS) that monitor and control high-wattage devices (e.g., through home automation systems [23]) and distributed generation.

This paper addresses this gap by introducing and analysing MaDIoT 3.0 attacks, a new class of coordinated cyberattacks that simultaneously target high-wattage IoT demand devices and DERs. As Figure 1 depicts, this concept represents an evolution of the original MaDIoT attack (MaDIoT 1.0) proposed by Soltan et al. [4], and the more sophisticated MaDIoT 2.0 variant by Shekari et al. [24], which assumed advanced attacker knowledge. In contrast, MaDIoT 3.0 explores the compounded effects of disrupting both demand and generation resources, reflecting a potentially more damaging threat scenario. MaDIoT 2.0 attacks are out of the scope of this paper because the assumption that the attacker has advanced knowledge about the system model and parameters, and access to dispatch information, is a strong hypothesis, since this information is usually well protected by the system operator.

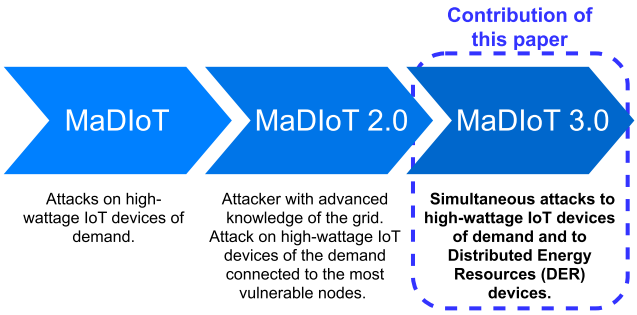

FIGURE 1. Evolution of MaDIoT attacks. MaDIoT 3.0 attacks are first explored in this paper.

The objective of this paper is to answer the following Research Questions (RQ) that, to the best of authors' knowledge, are not addressed in the literature:

RQ1: How does the presence of distributed solar PV generation affect the success of MaDIoT 1.0 attacks?

RQ2: What is the success and impact of MaDIoT 3.0 attacks compared to MaDIoT 1.0 attacks in the same system model?

To answer these questions, this article provides:

- A detailed analysis of the success and impact of MaDIoT 1.0 attacks in a new version of the PST-16 model that includes distributed solar PV generation in one area, enabling the assessment of how DERs influence the outcomes of such attacks. In this paper, an attack is considered successful if it manages to activate at least one electrical protection, which would disconnect loads or generators from the system.
- The definition and assessment of the success and impact of MaDIoT 3.0 attacks, which combine demand-side and DER-side attacks. To the best of the authors' knowledge, this is the first study to explore such coordinated attacks. Multiple scenarios are analysed, including multi-area and distributed demand attacks, expanding previous related research.

This paper is organised as follows. Section II first describes the modifications made to the PST-16 for the analysis in this paper (detailed in Appendix A), the protections considered, the adversary model, and the attack model and simulation scenarios. Section III presents and discusses the results obtained and Section IV outlines some possible measures to minimise the risk and impact of attacks. Finally, Section V draws conclusions.

II. MATERIALS AND METHODS

This section describes the assumptions, characteristics, and scenarios for the analysis.

A. TEST SYSTEM

In this paper, the PST-16 Benchmark System [25] is used for the analysis. The base PST-16 PowerFactory system model is available as part of the supplementary material in [25]. This system consists of three areas (A, B, C) and 66 buses with a total base load of 15565 MW active power and 2225 Mvar reactive power. The electrical frequency is 50 Hz, since it represents a simplified version of the European system. Areas A, B, and C represent north, central, and southern Europe, respectively [13]. The demand in area C (7465 MW) is greater than its generation capacity (6125 MW), so it needs power imports from A and B through two lines. Line A-C has a capacity of 1572 MVA and line B-C has a capacity of 2476 MVA.

This system implements the constant impedance load model and no changes were made to the models of bulk generators (i.e., nuclear, hydro, and coal) [25].

For the analysis of the impact of MaDIoT 3.0 attacks on the system, distributed solar Photovoltaic (PV) generation has been included in area C to buses that only have loads connected (no bulk generation), so that this generation is used for self-consumption within the node. Area C was selected because of:

a) Its representation of southern Europe in the PST-16 benchmark model. Spain's available data on distributed solar PV penetration was extrapolated (details in Appendix A).
b) Its mismatch between active load and maximum bulk generation capacity. Area C has less local generation capacity than other areas.
c) The moderate success ratio of MaDIoT 1.0 attacks obtained by [13] for this area. This allows for a better comparison of the impact of the attack when considering solar PV generation.

Figure 2 shows a simplified diagram of area C with the placement of distributed solar PV generation.

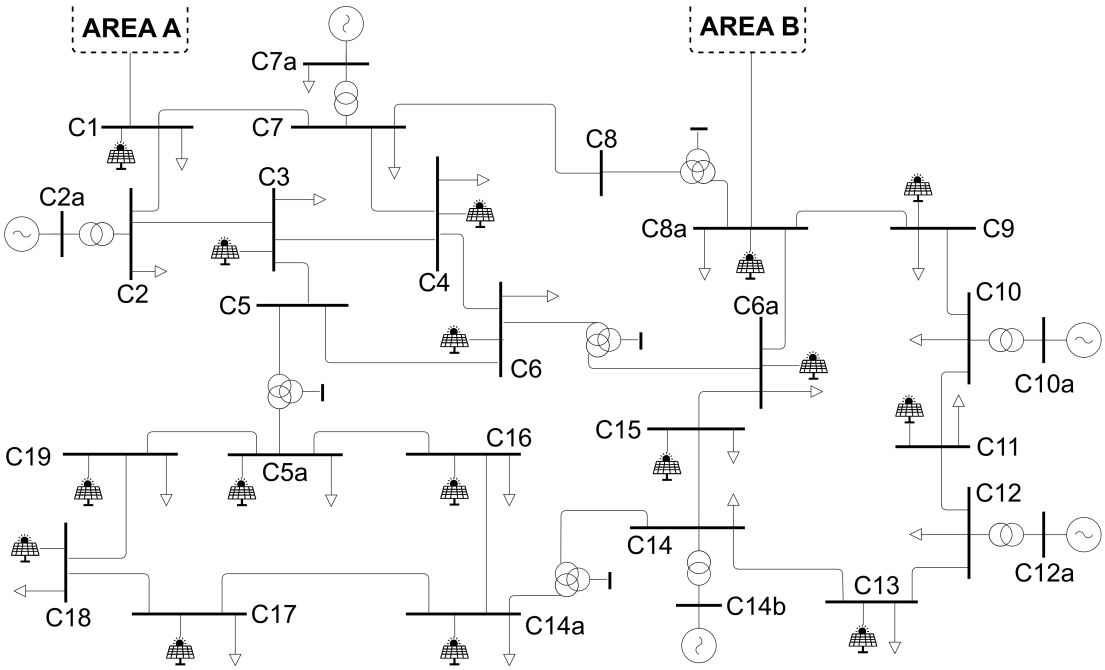

FIGURE 2. **Simplified diagram of area C in the PST-16 system with distributed solar PV included.**

The penetration degree of DER that is applied in this paper corresponds to the one estimated for Spain for the year 2030 (10% of the demand supplied by distributed solar PV generation). Since area C represents the South of Europe, this value was calculated by extrapolating actual data about solar PV generation connected to up to 145kV in Spain.

To estimate the penetration level of distributed solar PV generation in Spain in 2030, data updated by the Spanish regulator in March 2023 [26] has been used. The expected increase for 2030 is estimated by using information published by the Spanish Transmission System Operator (TSO) (i.e., *Red Eléctrica de España*) on the generation that has permission and is awaiting for connection to the distribution network; it is safe to assume that this generation will be operational by 2030 [27]. Based on this, it is estimated that by 2030 the penetration level of distributed solar PV generation will be 10%. Appendix A describes how the estimated value of 10% has been obtained, and Table 11 in the appendix shows the solar PV capacity that is connected to each bus in area C, summing up 546.5 MW. For simplicity, this generation has been represented within PowerFactory by means of *static generator* models with constant reactive power control. Since DER is included, the bulk generation has to decrease. It was assumed that the penetration of distributed solar PV generation in Area C displaces two conventional generation units, while the remaining bulk generation (23 units in Area C) maintains its maximum power output unchanged.

B. PROTECTIONS

Four protection types are considered: overvoltage protections, undervoltage protections, an Under-Frequency Load Shedding (UFLS) scheme, and an Over-Frequency Generator Rejection (OFGR) protection.

1) OVERVOLTAGE AND UNDERVOLTAGE PROTECTIONS

These protections disconnect loads when the voltage exceeds (F59 phase overvoltage protection) or is below (F27 phase undervoltage protection) a predetermined value. Overvoltage protections actuate when voltage exceeds 1.1 p.u for 10s, whereas undervoltage protections trip when voltage is below 0.85 p.u for 10s.

2) UFLS PROTECTION

This protection scheme gradually disconnects loads from the system as the frequency drops below certain levels, as shown by Table 1.

TABLE 1. **UFLS scheme applied; (frequency vs. load to be shed).**

Frequency Threshold (Hz)	49	48.8	48.6	48.4	48.2	48
Load-shed (%)	5	5	10	10	10	10

3) OFGR PROTECTION

To protect generators, this protection is activated when the frequency measured on the generator bus reaches 51.7 Hz, similar to that used in [8] and [13]. These protections disconnect the corresponding generator from the power system.

C. CRITERIA for ATTACK SUCCESS

As in [13], the attack is considered successful if, at the end of the simulation, any loads have been disconnected due to

UFLS, overvoltage, or undervoltage protections or if any generators have been disconnected due to OFGR protections. This criterion is similar to that in [7]. Therefore, to measure the success in each scenario, the success ratio is calculated as indicated by Equation 1.

$$\text{Success ratio} = \frac{\text{\# of successful attacks}}{\text{\# of attacks simulated}} \tag{1}$$

D. ADVERSARY MODEL

Table 2 illustrates the adversary model based on the guidelines provided by [28]. The adversary's knowledge is assumed to be limited, and they do not have physical access to the assets (referred to as non-possession adversary access). The attacks involve targeting high-wattage IoT devices under MaDIoT 1.0 attacks, activating them (1 bot = 3kW) and targeting solar PV generators under MaDIoT 3.0 attacks, disconnecting them from the system. The attacker is considered to possess significant resources, tools, and skills to execute the attack (classified as class II in [28]). It is important to note that, in this paper, the attacker is assumed to have compromised the devices and installed malware for command and control, allowing them to manipulate a large number of devices.

TABLE 2. Considered Manipulation of Demand through IoT (MaDIoT) adversary model based on guidelines by [28].

	Attack Model
Adversary knowledge	Oblivious
Adversary access	Non-possession
Adversary specificity	Targeted attack
Adversary resources	Class II

E. ATTACK MODEL AND SIMULATION SCENARIOS

The attack model for a MaDIoT 3.0 attack is presented in Table 3, based on the guidelines by [28]. This model is similar to the one for MaDIoT 1.0 attacks [13], [28]. However, control servers of DER could also be part of compromised assets, and attack techniques would also include *"module firmware"* to modify the control objectives of DER inverters. The functional level of the attack would be 1 (manipulation of control networks) or 2 (local networks overseeing processes).

Based on the adversary and attack model, a MaDIoT 3.0 attack would involve three steps: (1) identification and scanning of vulnerable IoT, DER devices, and related control and communication systems using known exploits or default credentials; (2) installation of malware or remote access trojans (RATs) to establish a botnet; and (3) coordinated activation or disconnection of devices via command-and-control (C2) servers. The attacker does not require real-time grid data but relies on general knowledge of device types.

Therefore, the attacker can initiate a MaDIoT 3.0 attack by sending commands to IoT devices to increase demand

TABLE 3. Considered MaDIoT 3.0 attack model based on the modelling guidelines by [28].

	Attack Model
Attack frequency	Iterative
Attack reproducibility and discoverability	Multiple-times
Attack functional level	Level 1 or 2
Attacked asset	Field controllers, human–machine interfaces, control servers
Attack techniques	Modify control logic, wireless compromise, and Denial-of-Service to the power grid, module firmware
Attack premise	Cyber: communications and protocols, and asset control commands

(e.g., turning on EV chargers), while simultaneously disconnecting DERs by issuing false control signals. This dual-action strategy is expected to increase the net load on the system, potentially triggering protection mechanisms or instability in the system. As indicated previously, the analysis in this paper does not focus on how the MaDIoT attack is performed, but on its impact on the power system assuming that an attacker managed to perform it.

Table 4 summarises the characteristics of the scenarios analysed in this paper. To improve the readability and understanding of the results in Section III, the name of each scenario follows the pattern depicted in Figure 3. On average, each scenario counts with ≈ 600 simulations (except for those scenarios considering area A and B, where the maximum number of combinations is smaller than 600).

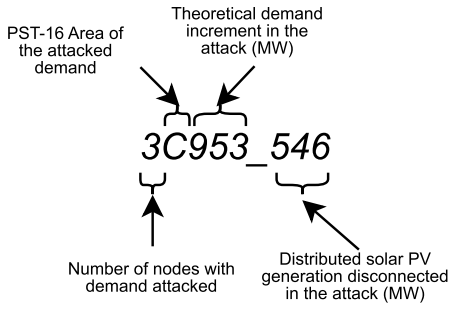

FIGURE 3. Explanation of the pattern followed for the names of the scenarios.

As in [13], the nodes to which the compromised loads are connected are selected randomly (uniform distribution) every time a simulation is executed, in a Monte Carlo-like way. The first eight scenarios in Table 4 consider that the loads attacked are distributed into three nodes, so that the increase in demand per node is significant during the attack. This allows us to compare the results with those obtained in [13]. Since the PST-16 system implements a constant impedance load model, the amount of demand increased by the attack

TABLE 4. Scenarios analysed for the PST-16 system with 546.5 MW (10% of demand in Area C) of distributed solar PV connected in Area C.

Scenario	Attack on demand				Attack on DER		Total
	Area	No. nodes	Botnet size	MW	Area	MW	(MW)
3C1500_0	C	3	500k	≈ 1500	NA	0	≈ 1500
3C1350_0	C	3	450k	≈ 1350	NA	0	≈ 1350
3C1200_0	C	3	400k	≈ 1200	NA	0	≈ 1200
3C953_546	C	3	318k	≈ 953	C	546.5	≈ 1500
3C1225_225	C	3	408k	≈ 1225	C	225	≈ 1450
3C525_525	C	3	175k	≈ 525	C	525	≈ 1050
3A953_546	A	3	318k	≈ 953	C	546.5	≈ 1500
3B953_546	B	3	318k	≈ 953	C	546.5	≈ 1500
6C1500_0	C	6	500k	≈ 1500	NA	0	≈ 1500
6C953_546	C	6	318k	≈ 953	C	546.5	≈ 1500
6C1500_546	C	6	500k	≈ 1500	C	546.5	≈ 2046

would be theoretical: the effective one in the simulation will depend on the behaviour of voltages. The impact on the power system is expected to decrease when the attack is spread across a larger number of nodes while maintaining the same botnet size; to assess the effect of this, the last three scenarios double the number of nodes involved to six.

Regarding the attack to DER, the simulation program selects the nodes whose DER power, when aggregated, is equal to the indicated value in the scenario. This means that there are no partial disconnections of DER within the same bus: if the bus is selected, all its DER are disconnected in the attack.

The first three scenarios (3C1500_0, 3C1350_0, and 3C1200_0) aim to evaluate the impact of MaDIoT 1.0 attacks (i.e., only demand is compromised) on the system with distributed solar PV generation. Since the connection of DER modifies the initial state of the system from the one used in [13], a different response to the attack and different success ratios can be expected.

The next three scenarios (3C953_546, 3C1225_225, and 3C525_525) allow the analysis of the impact of MaDIoT 3.0 attacks that combine demand and DER attacks performed at the same time. This means that the attacker manages to increase the demand and, at the same time, disconnects distributed solar PV generation.

In addition to this, five additional scenarios are considered to gain additional insight on the impact of MaDIoT 3.0 attacks. Two scenarios (3A953_546 and 3B953_546) allow to analyse the impact when the compromised demand and the compromised DER do not belong to the same area. This may be the case if an attacker only managed to find and exploit vulnerabilities in technologies, systems, or devices that were replicated more extensively in certain regions, such as Radio Ripple Control technologies in central Europe [21], [22]. The remaining three scenarios (6C1500_0, 6C953_546 and 6C1500_546) allow to analyse the impact of doubling the number of nodes attacked while keeping the botnet size invariant.

DER-only attacks (e.g., 3C0_546) are discarded from the analysis, since the disconnection of all the DER connected (546.5 MW) would not be enough for the attack to activate protections in the system, having a null success ratio, based on the results in [13] when performing MaDIoT 1.0 attacks to area C of PST-16 without DER.

TABLE 5. Hypothesis test for the success ratio in the base PST-16 system without DER (π_1) and the success ratio in the PST-16 system with DER (π_2).

$H_0 : \pi_1 = \pi_2$
$H_1 : \pi_1 < \pi_2$

Scenario	P-value
3C1200_0	0.026
3C1350_0	$2.27e-07$
3C1500_0	$7.40e-05$

III. RESULTS

This section presents the results when simulating the attack scenarios defined in Table 4 to answer the two RQs presented in the introduction of this paper.

A. RQ1: HOW DOES the PRESENCE of DISTRIBUTED SOLAR PV GENERATION AFFECT the SUCCESS of MaDIoT 1.0 ATTACKS?

To answer this question, the success ratio of MaDIoT 1.0 attacks (only demand is compromised) is analysed when the PST-16 system model includes DER generation and when it does not (i.e., original PST-16 model).

Figure 4 shows the success ratios of MaDIoT attacks in scenarios 3C1500_0, 3C1350_0, and 3C1200_0 compared to the success ratios obtained for the base PST-16 system model (without distributed solar PV connected) in [13].

It can be seen in Figure 4 that, for the three scenarios, the success ratio of MaDIoT 1.0 attacks in the system with distributed solar PV generation connected in area C is significantly lower than in the system with only bulk generation. This is statistically validated with a significance of 5% by the hypothesis test results shown in Table 5.

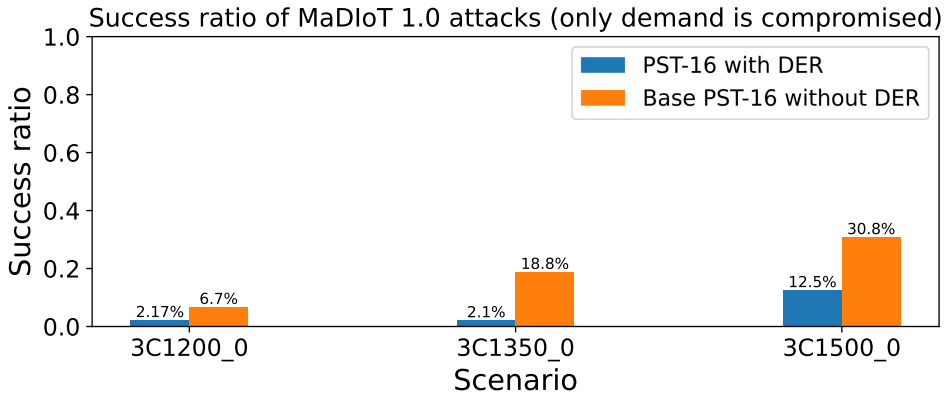

FIGURE 4. Success ratio of MaDIoT 1.0 attacks (demand compromised) in the PST-16 system with and without DER.

The success ratio only becomes relevant when 500k bots are attacked (3C1500_0), which constitutes a significant demand increment.

While it is true that replacing synchronous bulk generators with inverter-based DERs reduces system inertia, previous research has shown that MaDIoT 1.0 attacks in area C mainly affects generators' rotors and voltage dynamics [13]. This suggests that inertia is not the dominant factor that influences the outcome of the attacks in area C of the PST-16 system. Inertia primarily affects the power system's ability to resist rapid frequency deviations. However, an overview of the power system dynamics in the scenarios for the PST-16 system with DER indicates that the available synchronous generation is sufficient to stabilise the frequency within acceptable limits after the attack and frequency-related protections are not triggered.

Therefore, in the PST-16 system with DER, the instability appears to be related to the voltage and rotor angle dynamics, as it was the case for the original PST-16 without DER. Figure 5 shows that the connection of DER with constant reactive power control in area C increases the voltages of the nodes (average increase of 0.99%), putting the system in a better initial state to face the attack. This improved voltage level likely contributes to the lower success ratio observed in the DER-integrated system.

However, the success ratio may not be indicative of the impact of the attack: low success ratios could represent critical consequences (e.g., full blackout of the system) while high success ratios could represent a minor effect (e.g., just one protection activated). To gain an understanding of the magnitude of the attack's impact on the PST-16 system with DER, the simulated case with the most significant effect is analysed.

Figure 6 plots the frequency (Hz), the voltages (p.u), and the relative rotor angle (degrees) of generators in area C (with respect to the reference generator) against time when facing an attack defined for scenario 3C1500_0. The time of the attack (t = 0.5 s) is indicated by "*" in the x-axis. For the

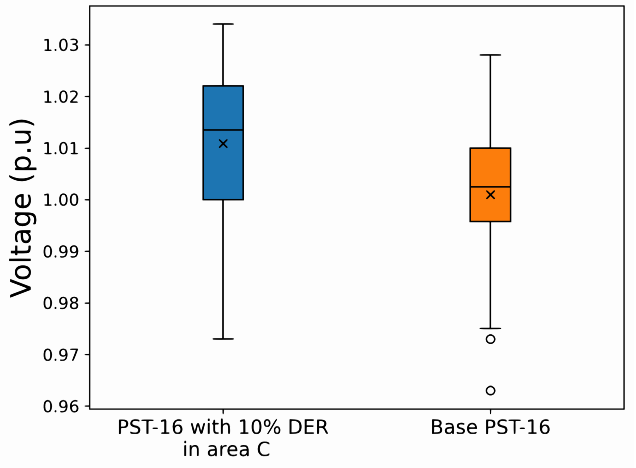

FIGURE 5. Comparison of bus voltages in area C when DER is connected.

frequency and voltages, only the information for five buses is plotted, including the buses to which the attacked loads are connected (loads 27, 30 and 34 connected to buses C13, C14a and C16, respectively), to keep the figure visually simple. Regarding the relative rotor angle, only three generators of area C are represented.

The results in Figure 6 demonstrate that the attack has a small effect on frequencies because the system has enough generation capacity. Frequencies slightly drop below 50 Hz for a few seconds before returning to the nominal value.

On the contrary, the voltage magnitudes of the targeted buses progressively decrease. The voltage magnitude of bus C13 falls below the limit of the voltage protection (0.85 pu) by $t \approx 6s$, resulting in undervoltage load shedding. The initially destabilizing impact of the attack on the voltage can also be observed in the rotor angles as shown in the bottom plot of Figure 6. The rotor angles of the generators of area C start diverging with respect to the reference generator right after the attack, accompanying the progressive decrease in

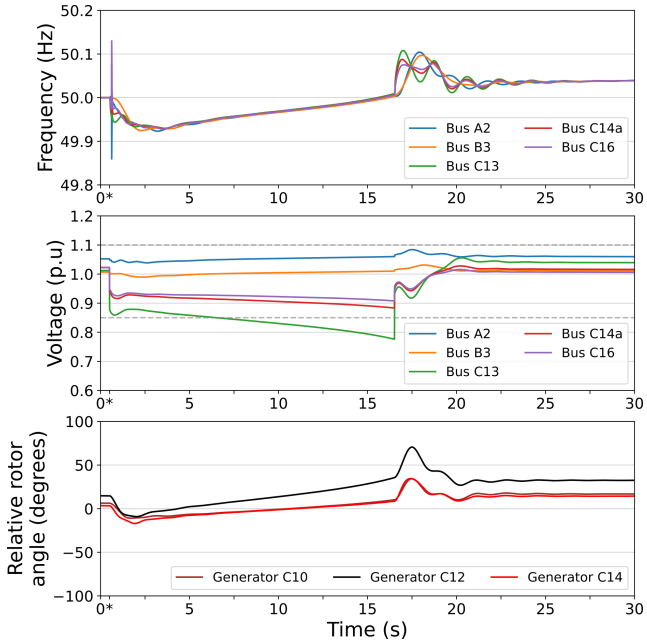

FIGURE 6. **Frequency, voltages, and relative rotor angle of generators in scenario 3C1500_0. Simulation run with the greatest impact. Attack at t=0.5s (indicated by *).**

the voltages of the area. The undervoltage load disconnection of 600 MW by $t \approx 16s$ achieves stopping the voltage decrease in particular and stabilizing the system in general. The load disconnection brings voltage magnitudes back within normal operation values. Steady state frequency remains slightly above 50 Hz due to the absence of a secondary control. OFGR protections do not need to actuate. In this case, by the end of the simulation the systems ends up with 188 MW less demand than before the attack (1.2% decrease). This is a much lower impact than the one presented in [13] for the system without DER, where the demand decreased 20% with respect to the initial demand.

In addition to this case, to validate this insight, a case has been simulated in which the same loads that were attacked in the highest-impact case in [13] are targeted for the system with DER; the results obtained show that the attack would not be successful (i.e., no protections were activated) under these new conditions.

However, when simulating the case presented in Figure 6 in the base PST-16 system without DER, the attack is successful and causes the disconnection of $\approx 2GW$ of generation and the disconnection of more than 2GW of demand, decreasing the demand of the system in $\approx$ 13% with respect to the initial demand. This means that the presence of only 546 MW of distributed solar PV in area C in substitution of bulk generation units has a great positive effect on the stability of the PST-16 system when facing MaDIoT 1.0 attacks.

In other words, MaDIoT attack studies should consider the increasing presence of distributed solar PV generation to generate meaningful results.

B. RQ2: WHAT IS the SUCCESS AND IMPACT of MaDIoT 3.0 ATTACKS COMPARED to MaDIoT 1.0 ATTACKS in the SAME SYSTEM MODEL?

Once the impact of distributed solar PV generation on the success ratio of MaDIoT 1.0 attacks has been analysed, the impact of performing combined attacks targeting high-wattage IoT demand and solar PV inverters (MaDIoT 3.0 attacks) is assessed and compared against MaDIoT 1.0 results in the PST-16 system with DER.

Table 6 shows the success ratio of MaDIoT 3.0 attack scenarios and their confidence interval for $\alpha = 0.1$. Scenario 3C953_546 just presents 2% of successful attacks. This is lower than the success ratio obtained for scenario 3C1500_0 (12.5%), despite both are equivalent in terms of total power affected ($\approx$ $1500MW$). This means that the amount of demand attacked, distributed in just three nodes of area C, has a greater influence on the success ratio of the attack than attacking all the DER connected to area C (546.5 MW). This can also be appreciated in scenario 3C525_525, with a null success ratio, and in scenario 3C1225_225, where success slightly increases when increasing the demand attacked. In these scenarios, while demand attacks are focused on three nodes, the DER that are attacked are distributed along area C so they have less impact on the probability of success for the attack. From a physical point of view, large voltage decreases in a few nodes affects more negatively to the system than small voltage decreases in many nodes.

TABLE 6. **Success ratio of MaDIoT 3.0 attacks on area C.**

Scenario	Success ratio	Confidence interval ($\alpha = 0.1$)
3C953_546	2%	[1.2% ; 2.8%]
3C1225_225	2.97%	[2.3% ; 3.67%]
3C525_525	0%	[0% ; 0.99%]

To analyse the perturbation that MaDIoT 3.0 attacks cause to the system in these scenarios, subfigures 7a and 7b show the frequency, voltages, and relative rotor angle of generators for the highest impact cases of scenarios 3C953_546 and 3C1225_225, respectively. A case for 3C525_525 was not plotted due to the lack of success of MaDIoT 3.0 in that scenario.

Both cases depicted by subfigures 7a and 7b show a similar perturbation in the system after a MaDIoT 3.0 attack. In terms of frequency, the mismatch between demand and generation caused by the attack provokes some small oscillations in the electrical frequency registered in the buses, not enough for the activation of frequency protections. As the attack increases power demand and disconnects DER, voltages of the buses will drop depending on their proximity to the compromised assets. Those buses that provide connection to compromised loads and solar PVs may experience greater voltage drops, which in some cases cause the activation of the assigned undervoltage protections after ten seconds, as can be appreciated in 7a and 7b. In the 3C953_546 case,

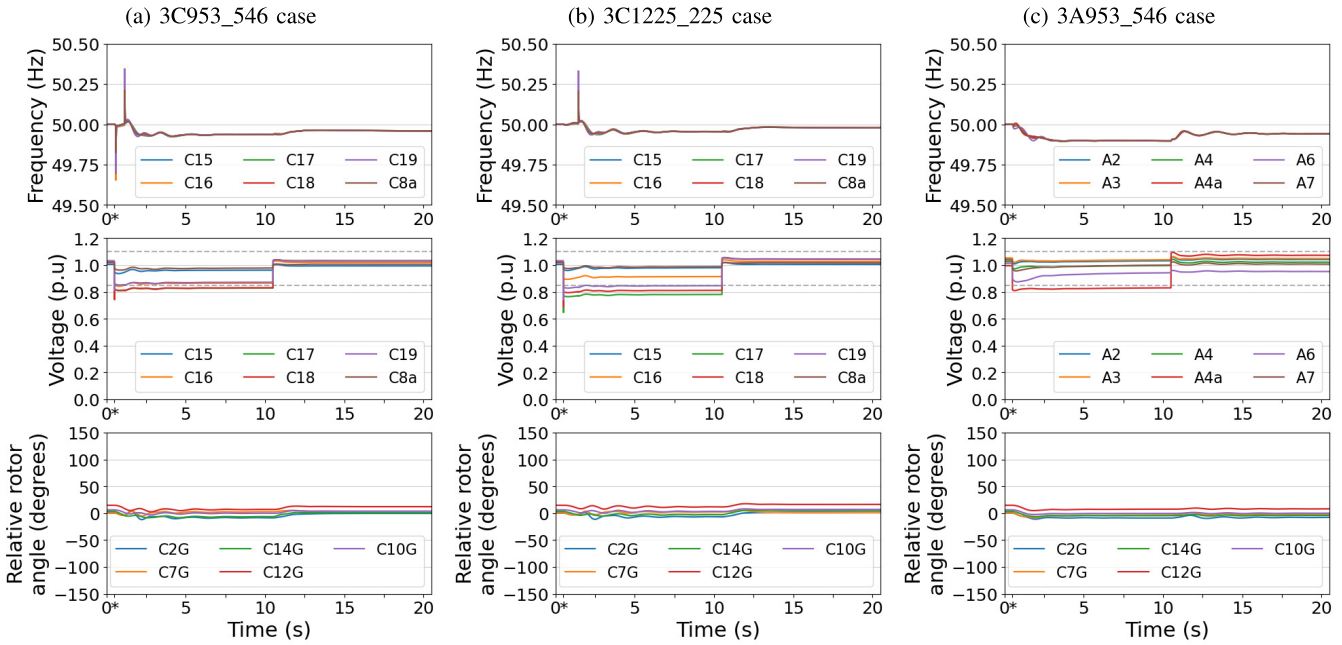

FIGURE 7. Frequency, voltages, and relative rotor angle of generators for the highest impact cases of scenarios 3C953_546 (a), 3C1225_225 (b), 3A953_546 (c).

125 MW ($\approx$ 0.8% of initial demand) are disconnected by the undervoltage protections; in the 3C1225_225, 105 MWs ($\approx$ 0.7%) are disconnected. As opposite to the MaDIoT 1.0 case analysed in the previous section (Figure 6), in these cases (3C953_546 and 3C1225_225) no voltage instability is appreciated in the voltage plot, which is also in line with what is shown by the relative rotor angle plot. Although there are some oscillations in the relative rotor angle of the generators in the area during the first 4-5 seconds after the attack, they become stable before and after the activation of the undervoltage protections, indicating that the available generation is able to keep voltages stable. Despite the fact that the theoretical magnitude of the attack is practically the same in the analysed MaDIoT 1.0 and 3.0 cases, the different contribution of loads and DER to the attack is behind the different behaviour of the system, showing the predominant effect of the amount of compromised demand on the impact of the attack.

The scenarios in Table 6 consider that the compromised demand is in the same areas as the attacked DER. However, apart from the DER in area C, an attacker may only have access to high-wattage IoT devices of the demand of other areas (A and B) for different reasons (e.g., socioeconomic aspects, better replicability of the systems, etc.). This arises the question of what would happen if compromised demand and DER are not in the same area in a MaDIoT 3.0 attack. To assess this, Table 7 shows the success ratio of MaDIoT 3.0 attacks when the targeted demand is in different areas of the system (A, B or C) while the targeted DER remains in area C. The three scenarios define attacks on the same amount of demand and DER.

TABLE 7. Success ratio of MaDIoT 3.0 attacks on different areas.

Scenario	Success ratio	Confidence interval ($\alpha = 0.1$)
3A953_546	5.95%	Exact
3B953_546	0%	Exact
3C953_546	2%	[1.2% ; 2.8%]

Attacks on demand of areas A and C have different success ratios (5.95% and 2%, respectively). However, in terms of impact, the perturbation caused in the 3A953_546 is similar to when the demand attack takes place in area C. Subfigure 7c shows the frequency, voltages, and relative rotor angle of generators for the highest impact case of scenario 3A953_546. Despite the frequency drop is more noticeable, it is still within the security margin before the activation of frequency protections. Some undervoltage protections are activated (disconnecting 200 MW, $\approx$ 1.3%), but voltages and rotor angles remain stable. Therefore, scenarios 3A953_546 and 3C953_546 are found similar in terms of impact. This is explained by the fact that, in the initial conditions of the PST-16 system, area C greatly depends on the support of area A to satisfy its demand: if local demand in area A increases as a result of an attack, this support is reduced. This is in line with the observations of previous research [13], where area A presented a high success ratio for MaDIoT 1.0 attacks due to its initial voltage conditions, turning it into a vulnerable area for this type of attacks.

However, if the attacked demand is in area B, the success ratio based on the simulated attacks is 0%, having null impact. Therefore, performing multiple-area MaDIoT 3.0 attacks do

not significantly increase the success ratio nor the impact in the PST-16 system under the analysed conditions.

Finally, it should be considered that the attacker may have access to the same amount of demand bots but distributed among more nodes in the system. For this, the success ratio of MaDIoT 3.0 attacks is evaluated when increasing from three to six the number of nodes to which the attacked demand is connected. This would be the case if the vulnerable high-wattage IoT devices are more distributed along area C (i.e., better replicability in this area). This also allows to slightly equate the conditions of the attacked demand to the conditions of the attacked DER, which was identified above as one of the main causes for the different impact of the two targets. Table 8 shows the success ratios (and their confidence interval) for scenarios 6C1500_0, 6C1500_546 and 6C953_546.

TABLE 8. Success ratio of MaDIoT 3.0 attacks when considering six buses for the attacked demand.

Scenario	Success ratio	Confidence interval ($\alpha = 0.1$)
6C1500_0	0%	[0% ; 0.27%]
6C1500_546	38.8%	[36.2% ; 41.2%]
6C953_546	0%	[0% ; 0.24%]

It is remarkable that merely attacking demand in six nodes dilutes the success ratio to 0%, compared to the 12.5% obtained when considering three nodes (3C1500_0 in Figure 4). This confirms that the large voltage decrease caused by increasing the demand on a few nodes has a greater impact than a smaller voltage decrease in many nodes. To increase the success ratio, it should be combined with attacks to the DER to increase the impact on voltages, as scenario 6C1500_546 shows. In this case, less demand per node is compromised (but in more nodes), and all the DER is attacked, achieving a success ratio of 38.8% for a theoretical attack magnitude of $\approx 2GW$. The impact also increases significantly with respect to other MaDIoT 3.0 scenarios analysed: in the worst case simulated in scenario 6C1500_546, whose dynamics are shown in Figure 8, generators are unable to keep their relative rotor angle constant, causing a voltage collapse and the activation of OFGR protections (2.85 GW of generation get disconnected) and undervoltage and frequency protections of loads, which disconnect 2.29 GW ($\approx$ 15%) of the demand to protect the system. This could potentially lead to a wide area blackout in an actual power system.

The results presented in this section provide interesting scalability and replicability insights about the connection of DER to area C of the PST-16 system and its impact on MaDIoT attacks. MaDIoT 1.0 attacks do not replicate the success and impact when 10% DER is connected, mainly because the buses in area C have higher voltages as a consequence of this connection.

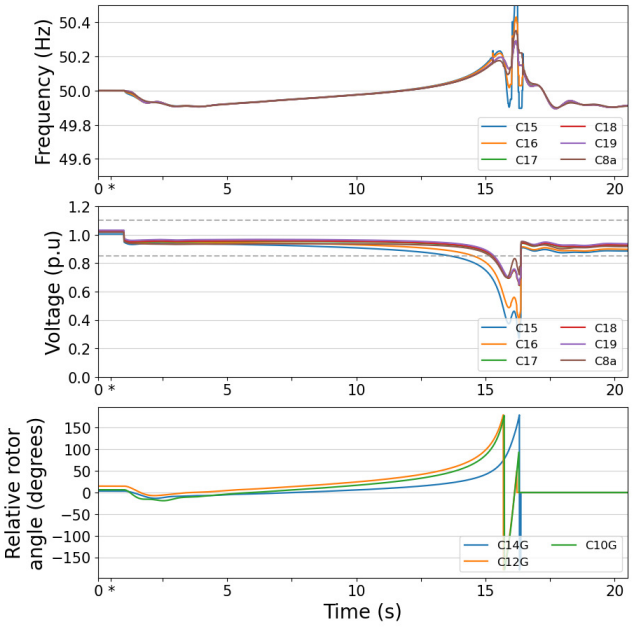

FIGURE 8. Frequency, voltages, and relative rotor angle of generators for the highest impact cases of scenarios 6C1500_546.

When performing MaDIoT 3.0 attacks in the PST-16 system, it was observed that the amount of demand attacked had a greater influence on the success ratio than the attacked DER, although the latter was relevant to achieve some success. On the other hand, attacking the demand in areas different from where DER is attacked would not increase the success ratio of the attack. In the same way, distributing the attacked demand between more buses would significantly decrease the success ratio, unless larger attacks are carried out.

IV. COUNTER MEASURES

Although it is impossible to eliminate the risk of suffering a MaDIoT-type attack, the adoption of some measures could significantly help to minimise it.

The most basic measure is to improve the security level of IoT devices by design. Especially for IoT devices at the consumer level, manufacturers usually do not add many security features to their products, which is combined with the lack of knowledge of most users about adopting good cybersecurity practices to properly protect their devices [29]. For DER devices, more security regulation should be developed [30].

In Europe, the European Cybersecurity Certification scheme (EUCC) [31] (adopted in 2024) sets some minimum requirements to certify devices in terms of cybersecurity, including compliance with international standards such as the Common Criteria for Information Technology Security Evaluation (ISO 15408), the selection of an independent accreditation body, the proved capacity of certification holders to report vulnerabilities and have vulnerability management and disclosure procedures defined, and the development

of a penalty system if entities fail to comply with security requirements.

To minimise the risk of being involved in a MaDIoT attack, any software and firmware updates of devices must be cryptographically verifiable [32] and have the possibility of a roll-back firmware update [16]. User authentication and role-based access control should be implemented, together with data encryption [16], [18]. Such measures would not negatively affect the operation of DER, as Johnson et al. [33] demonstrate that network segmentation, encryption and the implementation of a Moving Target Defense (MTD) strategy would not have an impact on latency.

Distribution System Operator (DSO)s, given that they operate the systems to which IoT and DER devices are mostly connected, should develop and implement intrusion detection / prevention systems [18] by using advanced techniques/technologies such as deep learning [34], data-driven algorithms [35], edge computing [36] or preventive algorithms to avoid line failures [37].

In addition to this, collaboration between DSOs, TSOs, and other entities (e.g., DER operators) is essential to achieve systemic resilience and minimise the impact of the attacks. To create collective situational awareness and minimise the risk of cascading failures, detailed real-time information sharing is necessary, as well as a coordinated response. To this end, European normative is evolving to encourage information sharing and cyber incident communication initiatives, such as the Network and Information Security 2 (NIS2) Directive [38]. NIS2 Directive, which includes the energy sector within its scope, introduces more security requirements, the obligation to report incidents to the designated national entity, and more extensive enforcement measures. More focused on the electricity sector, the Network Code on Cybersecurity [39] (adopted in 2024) establishes minimum cybersecurity requirements, cross-border risk management processes, cybersecurity controls, a framework for sharing cybersecurity information, and the definition of roles and responsibilities of the stakeholders involved, among other measures.

V. CONCLUSION

High-wattage IoT devices at the consumer level of electricity grids, as well as devices responsible for managing DER, have the potential to become new points of vulnerability for cyber attacks.

In this paper, the replicability of MaDIoT attacks in the PST-16 system with distributed solar PV generation has been examined. Furthermore, the effects of MaDIoT 3.0 attacks have been investigated and introduced in this paper.

The results indicate that the inclusion of 10% distributed solar PV generation (replacing bulk generation units) with constant reactive power control led to an average increase in area voltages of approximately 1%. Because of this, the MaDIoT 1.0 attack resulted in reduced success and impact compared to same attack in the power system without distributed generation.

When it comes to MaDIoT 3.0 attacks, the demand had a more significant influence on the attack's success than the DER. This can be attributed to the varying concentration of the distributed solar PV. It was observed that distributing the attacked demand across more buses or targeting the demand in areas other than the one with the attacked DER would decrease the success ratio. Therefore, for Madiot 3.0 attacks, the deployment of vulnerable high-wattage IoT devices in a few nodes of the demand becomes more critical than compromising devices distributed within or between areas of the same system.

This study, like previous ones, faces a key limitation: it does not consider the dynamics and protection methods in large electricity distribution systems, nor how operators might respond in real time to these attacks. To overcome this, a model that combines transmission and distribution systems is needed, along with ample computational capacity. In addition, operational mitigation strategies need to be formulated and included. Studying to what extent the different DER control (e.g., grid following and grid forming, etc.) affects the response to MaDIoT 3.0 attacks, the implementation and analysis of countermeasures, and further analysis considering inter-area balance constitute another interesting future research.

VI. APPENDIX A
DISTRIBUTED SOLAR PV GENERATION IN THE PST-16 SYSTEM

The penetration of solar PV per voltage level in Spain on March 2023 is shown by Table 9 [26]. For the study, only the solar PV connected to < 145kV is considered (i.e., distributed solar PV).

TABLE 9. Installed capacity of Solar PV generation in Spain per voltage level. Date: March 2023. Source: [26].

Voltage (kV)	Solar PV Generation (GW)	% of solar PV
$0 \leq V < 1$	1.67	9.56%
$1 \leq V < 36$	2.92	16.72%
$145 \leq V \leq 400$	10.27	58.8%
$36 \leq V < 72.5$	1.31	7.50%
$72.5 \leq V < 145$	1.29	7.41%

By considering the current electricity generation capacity of Spain, and the generation that is pending its start-up, but that has the permission to connect to the system [27], the percentage of solar PV connected to $<$ 145kV over the total generation capacity can be estimated for both the years 2023 and 2030, when it is assumed that all this expected generation will be already connected. Table 10 shows this estimation for the years 2023 and 2030 in Spain.

5.96% and 9.79% of distributed solar PV penetration equals to 365 MW and 599 MW of the total generation capacity in area C of the PST-16 system model. Since only

TABLE 10. Estimated solar PV generation connected to < 145kV for the years 2023 and 2030 in Spain. Source: Own elaboration based on public data from [26] and [27].

Scenario	Solar PV<145kV		Total Generation Power (GW)
	(GW)	(%)	
2023	7.191	5.96	120.64
2030	24.65	9.79	251.904

the load buses which do not have bulk generation connected are considered for the deployment of distributed solar PV (see Figure 2), the total amount of demand to which distributed solar PV would be connected is 5.46 GW. Therefore, with these values in mind, the percentage of this demand that could be supplied by distributed solar PV would be 6.68% and 10.97% for 2023 and 2030, respectively. These values are rounded down to 5 and 10%. For the analysis presented in this paper, only the 2030 scenario is considered, with 10% of demand supplied by distributed solar PV.

Table 11 shows the distributed solar PV that would be connected to each load bus for the years 2023 and 2030.

TABLE 11. Distributed solar PV generation per bus of area C (PST-16).

Bus	2030 (10%)
C1	60MW
C3	60MW
C4	50MW
C5a	6MW
C6	50MW
C6a	60MW
C8a	50MW
C9	50MW
C11	40MW
C13	60MW
C14a	4MW
C15	50MW
C16	2MW
C17	1MW
C18	2MW
C19	1.5MW

ACKNOWLEDGMENT

Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them. The authors would like to thank Dr. Álvaro Cárdenas (University of California Santa Cruz) for his valuable feedback and comments about this work, which helped the authors to increase the clarity and quality of the article.

REFERENCES

[1] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable?" *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5099–5113, Nov. 2020.

[2] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed Internet-based load altering attacks against smart power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 667–674, Dec. 2011.

[3] M. Mahrukh and M. S. Thomas, "Load altering attacks- a review of impact and mitigation strategies," in *Proc. Int. Conf. Recent Adv. Electr., Electron. Digit. Healthcare Technol. (REEDCON)*, May 2023, pp. 397–402.

[4] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. 27th USENIX Security Symp.*, Aug. 2018, pp. 15–32.

[5] A. Dabrowski, J. Ullrich, and E. R. Weippl, "Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well," in *Proc. 33rd Annu. Comput. Secur. Appl. Conf.*, New York, NY, USA, Dec. 2017, pp. 303–314.

[6] Y. Dvorkin and S. Garg, "IoT-enabled distributed cyber-attacks on transmission and distribution grids," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2017, pp. 1–6.

[7] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2862–2872, Jul. 2018.

[8] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against IoT demand attacks," in *Proc. 28th USENIX Secur. Symp.*, 2019, pp. 1115–1132.

[9] S. Lakshminarayana, S. Adhikari, and C. Maple, "Analysis of IoT-based load altering attacks against power grids using the theory of second-order dynamical systems," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4415–4425, Sep. 2021.

[10] M. P. Goodridge, S. Lakshminarayana, and C. Few, "Analysis of load-altering attacks against power grids: A rare-event sampling approach," in *Proc. 17th Int. Conf. Probabilistic Methods Appl. Power Syst. (PMAPS)*, Jun. 2022, pp. 1–6.

[11] T. Shekari, C. Irvene, A. A. Cardenas, and R. Beyah, "MaMIoT: Manipulation of energy market leveraging high wattage IoT botnets," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2021, pp. 1338–1356.

[12] B. Singer et al., "Shedding light on inconsistencies in grid cybersecurity: Disconnects and recommendations," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2023, pp. 38–55.

[13] N. Rodríguez-Pérez, J. Matanza Domingo, L. Sigrist, J. L. Rueda Torres, and G. López López, "Confronting the threat: Analysis of the impact of MaDIoT attacks in two power system models," *Energies*, vol. 16, no. 23, p. 7732, Nov. 2023.

[14] K. Chan, Y. Kim, and J.-Y. Jo, "DER communication networks and their security issues," in *Proc. IEEE 12th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2022, pp. 0785–0790.

[15] D. J. Sebastian and A. Hahn, "Exploring emerging cybersecurity risks from network-connected DER devices," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2017, pp. 1–6.

[16] R. S. de Carvalho and D. Saleem, "Recommended functionalities for improving cybersecurity of distributed energy resources," in *Proc. Resilience Week (RWS)*, Nov. 2019, pp. 226–231.

[17] I. Zografopoulos, C. Konstantinou, N. G. Tsoutsos, D. Zhu, and R. Broadwater, "Security assessment and impact analysis of cyberattacks in integrated T&D power systems," in *Proc. 9th Workshop Model. Simul. Cyber-Physical Energy Syst.*, May 2021, pp. 1–7.

[18] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *IEEE Syst. J.*, vol. 17, no. 4, pp. 6695–6709, Dec. 2023.

[19] J. Ye et al., "A review of cyber-physical security for photovoltaic systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 11, no. 1, pp. 1121–1140, Mar. 2023.

[20] D. Goodin. (2025). *Researchers Say New Attack Could Take Down the European Power Grid. Ars Technica*. [Online]. Available: https://arstechnica.com/security/2025/01/could-hackers-use-new-attack-to-take-down-european-power-grid/

[21] M. Plenz, A. Stadler, and D. Schulz, "Mitigating grid peaks in E-Mobility charging a comparative evaluation of § 14a EnWG and priority-driven load reduction approaches," in *Proc. 13th Int. Conf. Renew. Energy Res. Appl. (ICRERA)*, Nov. 2024, pp. 917–923.

[22] S. Chen and G. Heilscher, "Integration of distributed PV into smart grids: A comprehensive analysis for Germany," *Energy Strategy Rev.*, vol. 55, Sep. 2024, Art. no. 101525.

[23] A. Sahu, K. Davis, H. Huang, A. Umunnakwe, S. Zonouz, and A. Goulart, "Design of next-generation cyber-physical energy management systems: Monitoring to mitigation," *IEEE Open Access J. Power Energy*, vol. 10, pp. 151–163, 2023.

[24] T. Shekari, A. A. Cardenas, and R. Beyah, "MaDIoT 2.0: Modern high-wattage IoT botnet attacks and defenses," in *Proc. USENIX Secur. Symp.*, 2022, pp. 3539–3556.

[25] J. L. Rueda, J. C. Cepeda, I. Erlich, A. W. Korai, and F. M. Gonzalez-Longatt, "Probabilistic approach for risk evaluation of oscillatory stability in power systems," in *Power Systems*, 2014, pp. 249–266.

[26] *Comisión Nacional De Los Mercados Y La Competencia (CNMC). Información Mensual De Estadísticas Sobre Producción De Energía Eléctrica a Partir De Renovables, Cogeneración Y Residuos*. Accessed: Jul. 6, 2023. [Online]. Available: https://www.cnmc.es

[27] *Consulta El Estado De Las Solicitudes*. Accessed: Jul. 6, 2023. [Online]. Available: https://www.ree.es/es/clientes/generador/acceso-conexion/conoce-el-estado-de-las-solicitudes

[28] 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. 29775–29818, 2021.

[29] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security evaluation of home-based IoT deployments," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Francisco, CA, USA, May 2019, pp. 1362–1380.

[30] D. J. S. Cardenas, A. Hahn, and C.-C. Liu, "Assessing cyber-physical risks of IoT-based energy devices in grid operations," *IEEE Access*, vol. 8, pp. 61161–61173, 2020.

[31] ENISA. (Oct. 2023). *Cybersecurity-security Requirements for ICT Product Certification*. [Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13382-Cybersecurity-security-requirements-for-ICT-product-certificationen

[32] N. Duan et al., "Mitigation strategies against cyberattacks on distributed energy resources," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2021, pp. 1–5.

[33] J. Johnson, I. Onunkwo, P. Cordeiro, B. J. Wright, N. Jacobs, and C. Lai, "Assessing DER network cybersecurity defences in a power-communication co-simulation environment," *IET Cyber-Physical Syst., Theory Appl.*, vol. 5, no. 3, pp. 274–282, Sep. 2020.

[34] L. Wang, L. Pepin, Y. Li, F. Miao, A. Herzberg, and P. Zhang, "Securing power distribution grid against power botnet attacks," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2019, pp. 1–5.

[35] S. Lakshminarayana, S. Sthapit, H. Jahangir, C. Maple, and H. V. Poor, "Data-driven detection and identification of IoT-enabled load-altering attacks in power grids," *IET Smart Grid*, vol. 5, no. 3, pp. 203–218, Jun. 2022.

[36] B. Shrestha and H. Lin, "Data-centric edge computing to defend power grids against IoT-based attacks," *Computer*, vol. 53, no. 5, pp. 35–43, May 2020.

[37] S. Soltan, P. Mittal, and H. V. Poor, "Protecting the grid against MAD attacks," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 3, pp. 1310–1326, Jul. 2020.

[38] (Dec. 2022). *Eu Directive 2022/2555 (nis 2 Directive)*. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555

[39] (Oct. 2023). *Eu Electricity Supply-sector-specific Rules on Cybersecurity (network Code)*. [Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13101-EU-electricity-supply-sector-specific-rules-on-cybersecurity-network-code-en