A Proactive Intrusion Detection and Mitigation System for Grid-Connected Photovoltaic Inverters

Fazel Mohammadi, *Senior Member, IEEE*, Rasoul Bok, and Mehrdad Saif, *Senior Member, IEEE*

***Abstract*—The breach of data confidentiality, integrity, and availability due to cyberattacks can adversely impact the operation of grid-connected Photovoltaic (PV) inverters. Detecting such attacks based on their signatures or behavior-based analytics and adopting corrective actions to prevent security breaches for grid-connected PV systems requires the implementation of an intelligent Intrusion Detection System (IDS). In this paper, a Proactive Intrusion Detection and Mitigation System (PIDMS) based on real-time stability boundary identification at the Point of Common Coupling (PCC) for grid-connected PV systems is presented to identify the potentially compromised grid-connected PV systems in Cyber-Physical Power and Energy Systems (CPPES). The proposed PIDMS correlates the variations in the active power and reactive power measurements to power grids voltage at the PCC in real-time and accurately identifies compromised grid-connected PV systems, and enhances the resilience of CPPES. The performance of the proposed PIDMS is validated through dynamic simulations under different operating conditions. The obtained results verify the applicability and effectiveness of the proposed PIDMS.**

***Index Terms*—Cyber resilience, cyber - physical power and energy systems (CPPES), cyberattacks, grid - connected photovoltaic (PV) systems, intrusion detection and mitigation.**

I. Introduction

THE data confidentiality, integrity, and availability of Photovoltaic (PV) systems can be ensured by continuous monitoring and accurate detection and identification of cyberattacks. Intrusion Detection Systems (IDSs) utilize the signature(s) and/or behavior(s) of PV systems to detect and identify cyberattacks in Cyber-Physical Power and Energy Systems (CPPES) [1], [2], [3]. Regardless of the operating mode of PV systems, i.e., grid-connected and/or islanded, the adverse impacts of cyberattacks with the aim of tampering with the PV systems' measurements and commands lead to transient voltage instability and lack of proper power management; thus, disruption of CPPES operation [4], [5], [6]. From a technical point of view, real-time monitoring and control of grid-connected PV systems require reliable wired or wireless communication infrastructure to allow for exchanging information, and therefore, PV systems are exposed to False Data Injection (FDI) and tampering attacks [7], [8], [9], [10]. Therefore, it is vital to design and implement an intrusion detection and mitigation system to protect CPPES against cyberattacks and prevent their detrimental consequences in CPPES operations.

Different strategies for detecting and identifying cyberattacks targeting grid-connected PV systems are investigated in the literature [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29]. In [11], the cybersecurity roadmaps for PV systems are summarized, and appropriate practices for enhancing their cyber resilience are provided. Three network-based defense strategies for PV systems, including network segmentation, encryption, and moving target defense in a virtualized environment, are investigated in [12]. In [13] and [14], the Flatness-Based Control (FBC) method for Voltage Source Converters (VSCs) is presented to minimize the impacts of the noise on the measurement feedback, making the system less vulnerable to sudden faults and malicious attacks. An adaptive resilient control strategy to mitigate FDI attacks on grid-forming converters is introduced in [15] to ensure synchronization using adaptive communication weights. A model-based cyberattack detection based on Harmonics State Space Matrix (H-Matrix) for VSCs in an islanded microgrid is investigated in [16]. In [17], the signature and behavior-based analysis methods are presented to detect malicious network activities in the PV inverter control system. Using Artificial Intelligence (AI)-based intrusion and malware detection systems is a promising approach to overcoming the complexity of cybersecurity and successfully mitigating cyberattacks [18], [19], [20]. The implementation of various data-driven methods, including Decision Tree (DT), K-Nearest Neighbor (KNN), Support Vector Machine (SVM), Artificial Neural Networks (ANN), Long Short-Term Memory (LSTM), and Convolutional Neural Networks (CNN), to validate the possibility of using

Manuscript received 11 May 2023; revised 9 July 2023; accepted 13 October 2023. Date of publication 23 October 2023; date of current version 6 November 2023. *(Corresponding author: Fazel Mohammadi.)*

Fazel Mohammadi is with the Electrical and Computer Engineering and Computer Science Department, University of New Haven, West Haven, CT 06516 USA (e-mail: fmohammadi@newhaven.edu, fazel.mohammadi@ieee.org).

Rasoul Bok is with the Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan 84156-83111, Iran (e-mail: rasool.bok@ec.iut.ac.ir).

Mehrdad Saif is with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON N9B 3P4, Canada (e-mail: msaif@uwindsor.ca).

Digital Object Identifier 10.1109/TICPS.2023.3326773

micro-PMU (μPMU) data to detect and diagnose malicious attacks targeting PV systems is investigated in [21]. An online high-dimensional data-driven approach is presented in [22] to detect and identify cyberattacks on PV inverters. In [23], the impacts of data integrity attacks on different control loops in a PV system are analyzed, and a data-driven method using μPMU data is presented to detect cyberattacks in the PV system. Various vulnerabilities with PV inverters are identified in [24], and mitigation strategies, including a Neural Networks (NN)-based intrusion detection system, are suggested. Furthermore, signal processing-based methods, including the dynamic watermarking approach [25] and perturbation-based FDI attack detection mechanism [26] are investigated. A Man-in-the-Middle (MITM) attack against the manufacturing message specification of IEC 61850 for PV systems is investigated in [27]. Additionally, the impacts of firmware modification attacks on PV inverters are mitigated using custom-built Hardware Performance Counters (HPCs) as Design-For-Security (DFS) primitives [28] and Blockchain technology [29].

Existing approaches have been rarely used to simultaneously detect and mitigate cyberattacks at the device level (power electronic converters). Therefore, it is required to develop a method to accurately and quickly detect and mitigate cyberattacks that can negatively impact both power electronic converters, such as grid-connected PV inverters, and other critical components in power grids. Based on the above-mentioned explanations and analyses, a Proactive Intrusion Detection and Mitigation System (PIDMS) based on real-time stability boundary identification at the Point of Common Coupling (PCC) for grid-connected PV systems is proposed in this paper to identify the potentially compromised grid-connected PV systems in CPPES. In this regard, a stability index is introduced to determine the operating regions of a two-stage transformerless grid-connected PV system in real-time by correlating the variations in the active power and reactive power measurements to power grids voltage at PCC. In addition, operational constraints related to the PV system, i.e., predefined minimum and maximum power generation limits of the PV array and minimum and maximum power of the PV inverter, are considered to identify the manipulated data. The proposed PIDMS is capable of detecting forged power injection set-points used for the PV controller and adopting corrective actions, i.e., restoring the PV controller operation with predefined power injection set-points, to ensure the stability of power grids at the PCC and enhance the resilience of CPPES. Various operating conditions are considered to assess and verify the performance of the proposed PIDMS using dynamic simulation. In summary, the main contributions of this paper are as follows:

1) Analyzing the impact of cyberattacks on the control signal set-points of the PV controller and voltage and current measurements at PCC.
2) Introducing a stability index by correlating the variations in the active power and reactive power measurements to power grids voltage at PCC.
3) Developing a PIDMS based on real-time stability boundary identification at PCC for a grid-connected PV system to detect cyberattacks and adopt corrective actions.

The rest of this paper is organized as follows: Section II presents the proposed PIDMS for a grid-connected PV system. The simulation and experimental results are presented in Section III. Finally, Section IV concludes this paper.

II. Descriptions of the Proposed PIDMS for a Grid-Connected PV System

The structure of a grid-connected PV system is shown in Fig. 1. The PV system is connected to power grids at a local PCC terminal, and the PV inverter follows the local PCC voltage imposed by power grids. There is a Thévenin equivalent circuit, representing the remaining components of power grids, seen by the grid-connected PV inverter, which can be determined based on the location of the grid-connected PV system and its distance to the power grids' feeder. The system consists of three layers, i.e., physical, cyber, and control layers. The physical layer includes all the physical components of the system, i.e., PV array, DC/DC power converter, DC/AC inverter, filter, etc. The operating set-points of the local PCC are assigned by the cyber layer to the control layer.

Taking Fig. 1 into account, the voltage at the i^{th} local PCC ($\vec{v}_{\text{PCC}_i}$) can be derived as follows:

$$\begin{aligned}\vec{v}_{\text{PCC}_i} &= \vec{v}_{\text{TH}_i} + Z_{\text{TH}_i}\vec{i}_{\text{PCC}_i}\\ &= \left|\left|V_{\text{PCC}_i}\right|\right|_2 \angle \delta_{\text{PCC}_i}\\ &= \gamma_i + j\lambda_i \end{aligned} \tag{1}$$

where $\vec{v}_{\text{TH}_i}$ and Z_{TH_i} are the Thévenin equivalent voltage and Thévenin series impedance seen by the i^{th} grid-connected PV inverter from its local PCC to the power grids' feeder, $\vec{i}_{\text{PCC}_i}$ is the injected current by the i^{th} grid-connected PV inverter into its local PCC. In addition, the voltage at the i^{th} local PCC can be represented by a voltage ℓ_2-norm $\left|\left|V_{\text{PCC}_i}\right|\right|_2$ and voltage phase angle δ_{PCC_i}, which forms a complex number as $\gamma_i + j\lambda_i$.

Similarly, the voltage of the power grids' feeder can be written as follows:

$$\begin{aligned}\vec{v}_{\text{TH}_i} &= \left|\left|V_{\text{TH}_i}\right|\right|_2 \angle \delta_{\text{TH}_i}\\ &= \left|\left|V_{\text{TH}_i}\right|\right|_2 \left(\cos(\delta_{\text{TH}_i}) + j\sin(\delta_{\text{TH}_i})\right)\end{aligned} \tag{2}$$

where $\left|\left|V_{\text{TH}_i}\right|\right|_2$ and δ_{TH_i} are the voltage ℓ_2-norm the voltage phase angle of the power grids' feeder, respectively.

It should be noted that $\vec{v}_{\text{TH}_i}$ depends on the active power (P) and reactive power (Q) injected to/absorbed from different nodes, i.e., $\vec{v}_{\text{TH}_i} = f(P_{\text{PCC}_{(i+1)}}, Q_{\text{PCC}_{(i+1)}}, \ldots, P_{\text{PCC}_n}, Q_{\text{PCC}_n})$, where n shows the number of nodes in power grids. Consequently, $\vec{v}_{\text{PCC}_i}$ can be correlated to the active and reactive power set-points. Additionally, $\vec{i}_{\text{PCC}_i}$ can be written as follows:

$$\vec{i}_{\text{PCC}_i} = \frac{S^*_{\text{PCC}_i}}{\vec{v}^*_{\text{PCC}_i}} = \frac{P_{\text{PCC}_i} - jQ_{\text{PCC}_i}}{\vec{v}^*_{\text{PCC}_i}} \tag{3}$$

where $\vec{v}^*_{\text{PCC}_i}$ is the complex conjugate of $\vec{v}_{\text{PCC}_i}$, and P_{PCC_i} and Q_{PCC_i} are the net active power and reactive power at the i^{th} local PCC.

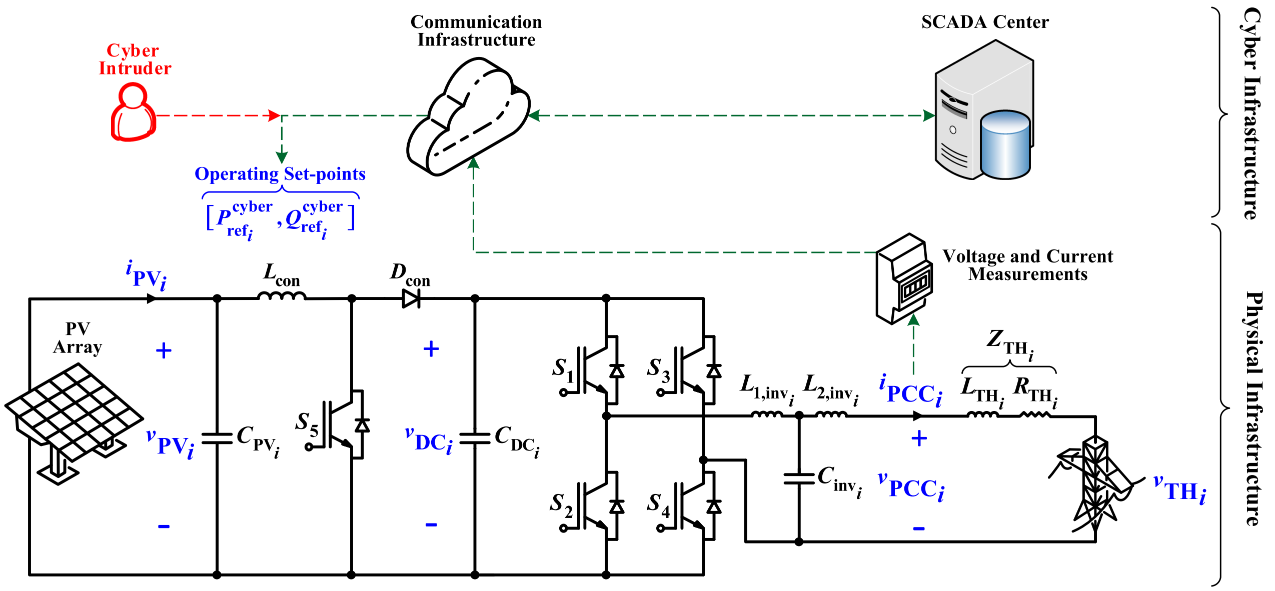


Fig. 1. Structure of a grid-connected PV system.

Therefore, (1) can be rewritten as follows:

$$\vec{v}_{\text{PCC}_i} = \vec{v}_{\text{TH}_i} + Z_{\text{TH}_i}\left(\frac{P_{\text{PCC}_i} - jQ_{\text{PCC}_i}}{\vec{v}^*_{\text{PCC}_i}}\right) \tag{4}$$

By multiplying (4) by $\vec{v}^*_{\text{PCC}_i}$ and considering $Z_{\text{TH}_i} = R_{\text{TH}_i} + jX_{\text{TH}_i}$, the following expression can be written.

$$\begin{aligned}\overbrace{\vec{v}_{\text{PCC}_i}\vec{v}^*_{\text{PCC}_i}}^{\gamma_i^2+\lambda_i^2} &= R_{\text{TH}_i}P_{\text{PCC}_i} + X_{\text{TH}_i}Q_{\text{PCC}_i}\\ &\quad + ||V_{\text{TH}_i}||_2\,(\gamma_i\cos(\delta_{\text{TH}_i}) + \lambda_i\sin(\delta_{\text{TH}_i}))\\ &\quad + j\Bigg(X_{\text{TH}_i}P_{\text{PCC}_i} - R_{\text{TH}_i}Q_{\text{PCC}_i}\\ &\quad + ||V_{\text{TH}_i}||_2\,(\gamma_i\sin(\delta_{\text{TH}_i}) - \lambda_i\cos(\delta_{\text{TH}_i}))\Bigg)\end{aligned} \tag{5}$$

where R_{TH_i} and X_{TH_i} are the resistance and reactance seen by the i^{th} grid-connected PV inverter from its local PCC, respectively.

Equation (5) comprises two parts, i.e., real and imaginary parts. Evidently,

$$\begin{cases}\gamma_i^2 + \lambda_i^2 = R_{\text{TH}_i}P_{\text{PCC}_i} + X_{\text{TH}_i}Q_{\text{PCC}_i}\\ \qquad + ||V_{\text{TH}_i}||_2\,(\gamma_i\cos(\delta_{\text{TH}_i}) + \lambda_i\sin(\delta_{\text{TH}_i}))\\ 0 = X_{\text{TH}_i}P_{\text{PCC}_i} - R_{\text{TH}_i}Q_{\text{PCC}_i}\\ \qquad + ||V_{\text{TH}_i}||_2\,(\gamma_i\sin(\delta_{\text{TH}_i}) - \lambda_i\cos(\delta_{\text{TH}_i}))\end{cases} \tag{6}$$

Equation (6) should be solved to determine γ_i and λ_i. In this regard, λ_i can be written in the form of γ_i, as follows:

$$\lambda_i = \frac{X_{\text{TH}_i}P_{\text{PCC}_i} - R_{\text{TH}_i}Q_{\text{PCC}_i}}{||V_{\text{TH}_i}||_2\cos(\delta_{\text{TH}_i})} + ||V_{\text{TH}_i}||_2\gamma_i\sin(\delta_{\text{TH}_i}) \tag{7}$$

Substituting for λ_i leads to the following expression.

$$\begin{aligned}&\gamma_i - \gamma_i\left(\frac{2\,(R_{\text{TH}_i}Q_{\text{PCC}_i} - X_{\text{TH}_i}P_{\text{PCC}_i})}{||V_{\text{TH}_i}||_2\sin(\delta_{\text{TH}_i})} + ||V_{\text{TH}_i}||_2\cos(\delta_{\text{TH}_i})\right)\\ &+ \left(\frac{X_{\text{TH}_i}P_{\text{PCC}_i} - R_{\text{TH}_i}Q_{\text{PCC}_i}}{||V_{\text{TH}_i}||_2}\right)^2\\ &- (R_{\text{TH}_i}P_{\text{PCC}_i} + X_{\text{TH}_i}Q_{\text{PCC}_i})\cos^2(\delta_{\text{TH}_i})\\ &- (X_{\text{TH}_i}P_{\text{PCC}_i} - R_{\text{TH}_i}Q_{\text{PCC}_i})\cos(\delta_{\text{TH}_i})\sin(\delta_{\text{TH}_i}) = 0\end{aligned} \tag{8}$$

Equation (8) is a quadratic equation with two roots, of which only its positive root is acceptable. This implies that if the grid-connected PV inverter does not inject active and reactive power at its local PCC, then, $\vec{v}_{\text{PCC}_i} = \vec{v}_{\text{TH}_i}$. Therefore,

$$\begin{aligned}\gamma_i = &\frac{||V_{\text{TH}_i}||_2}{2}\cos(\delta_{\text{TH}_i})\\ &+ \left(\frac{R_{\text{TH}_i}Q_{\text{PCC}_i} - X_{\text{TH}_i}P_{\text{PCC}_i}}{||V_{\text{TH}_i}||_2}\right)\sin(\delta_{\text{TH}_i})\\ &+ \Bigg[\frac{||V_{\text{TH}_i}||_2^2}{4}\cos^2(\delta_{\text{TH}_i}) - \left(\frac{X_{\text{TH}_i}P_{\text{PCC}_i} - R_{\text{TH}_i}Q_{\text{PCC}_i}}{||V_{\text{TH}_i}||_2}\right)^2\\ &+ \left(\frac{X_{\text{TH}_i}P_{\text{PCC}_i} - R_{\text{TH}_i}Q_{\text{PCC}_i}}{||V_{\text{TH}_i}||_2}\right)^2\sin^2(\delta_{\text{TH}_i})\\ &+ (R_{\text{TH}_i}P_{\text{PCC}_i} + X_{\text{TH}_i}Q_{\text{PCC}_i})\cos^2(\delta_{\text{TH}_i})\\ &+ (X_{\text{TH}_i}P_{\text{PCC}_i} - R_{\text{TH}_i}Q_{\text{PCC}_i})\sin(\delta_{\text{TH}_i})\cos(\delta_{\text{TH}_i})\Bigg]^{\frac{1}{2}}\end{aligned} \tag{9}$$

Accordingly,

$$\begin{aligned}\lambda_i = {} & \frac{||V_{\mathrm{TH}_i}||_2}{2}\sin(\delta_{\mathrm{TH}_i}) + \left(\frac{X_{\mathrm{TH}_i}P_{\mathrm{PCC}_i} - R_{\mathrm{TH}_i}Q_{\mathrm{PCC}_i}}{||V_{\mathrm{TH}_i}||_2\cos(\delta_{\mathrm{TH}_i})}\right)\\ & + \left(\frac{R_{\mathrm{TH}_i}Q_{\mathrm{PCC}_i} - X_{\mathrm{TH}_i}P_{\mathrm{PCC}_i}}{||V_{\mathrm{TH}_i}||_2\cos(\delta_{\mathrm{TH}_i})}\right)\sin^2(\delta_{\mathrm{TH}_i})\\ & + \tan(\delta_{\mathrm{TH}_i})\Bigg[\frac{||V_{\mathrm{TH}_i}||_2^2}{4}\cos^2(\delta_{\mathrm{TH}_i})\\ & - \left(\frac{X_{\mathrm{TH}_i}P_{\mathrm{PCC}_i} - R_{\mathrm{TH}_i}Q_{\mathrm{PCC}_i}}{||V_{\mathrm{TH}_i}||_2}\right)^2\\ & + \left(\frac{X_{\mathrm{TH}_i}P_{\mathrm{PCC}_i} - R_{\mathrm{TH}_i}Q_{\mathrm{PCC}_i}}{||V_{\mathrm{TH}_i}||_2}\right)^2\sin^2(\delta_{\mathrm{TH}_i})\\ & + (R_{\mathrm{TH}_i}P_{\mathrm{PCC}_i} + X_{\mathrm{TH}_i}Q_{\mathrm{PCC}_i})\cos^2(\delta_{\mathrm{TH}_i})\\ & + (X_{\mathrm{TH}_i}P_{\mathrm{PCC}_i} - R_{\mathrm{TH}_i}Q_{\mathrm{PCC}_i})\sin(\delta_{\mathrm{TH}_i})\cos(\delta_{\mathrm{TH}_i})\Bigg]^{\frac{1}{2}}\end{aligned} \tag{10}$$

The magnitude of the voltage at the i^{th} local PCC is a function of λ_i and γ_i such that $||\vec{v}_{\mathrm{PCC}_i}||_2 = (\lambda_i^2 + \gamma_i^2)^{\frac{1}{2}}$, which in turn determines the stability boundary of the voltage at the i^{th} local PCC. This also implies that the magnitude of the voltage at the i^{th} local PCC is impacted by both the set-points of the i^{th} local PCC and its nearby bus voltage. Consequently, the stability boundary of the i^{th} local PCC can be identified by projecting $||\vec{v}_{\mathrm{PCC}_i}||_2$ on the P_{PCC_i}–Q_{PCC_i} plane. Under normal operating conditions, $||\vec{v}_{\mathrm{PCC}_i}||_2$ should be between $0.8\ \mathrm{p.u.}$ and $1.2\ \mathrm{p.u.}$

Considering (9) and (10), a stability index, i.e., κ_i, at the i^{th} local PCC is defined as follows:

$$\begin{aligned}\kappa_i = {} & \frac{||V_{\mathrm{TH}_i}||_2^2}{4}\cos^2(\delta_{\mathrm{TH}_i}) - \left(\frac{X_{\mathrm{TH}_i}P_{\mathrm{PCC}_i} - R_{\mathrm{TH}_i}Q_{\mathrm{PCC}_i}}{||V_{\mathrm{TH}_i}||_2}\right)^2\\ & + \left(\frac{X_{\mathrm{TH}_i}P_{\mathrm{PCC}_i} - R_{\mathrm{TH}_i}Q_{\mathrm{PCC}_i}}{||V_{\mathrm{TH}_i}||_2}\right)^2\sin^2(\delta_{\mathrm{TH}_i})\\ & + (R_{\mathrm{TH}_i}P_{\mathrm{PCC}_i} + X_{\mathrm{TH}_i}Q_{\mathrm{PCC}_i})\cos^2(\delta_{\mathrm{TH}_i})\\ & + (X_{\mathrm{TH}_i}P_{\mathrm{PCC}_i} - R_{\mathrm{TH}_i}Q_{\mathrm{PCC}_i})\sin(\delta_{\mathrm{TH}_i})\cos(\delta_{\mathrm{TH}_i})\end{aligned} \tag{11}$$

The normal operating condition of the grid-connected PV inverter at the i^{th} local PCC is guaranteed, if and only if κ_i is a positive value, i.e., $\kappa_i > 0$.

Using the Clarke transformation, the active and reactive power at the i^{th} local PCC using its voltage and current in a stationary $\alpha\beta$ reference frame, i.e., $v_{\mathrm{PCC}_i}^{\alpha}$, $v_{\mathrm{PCC}_i}^{\beta}$, $i_{\mathrm{PCC}_i}^{\alpha}$, and $i_{\mathrm{PCC}_i}^{\beta}$, can be written as follows [30]:

$$\begin{cases} P_{\mathrm{PCC}_i} = \dfrac{1}{2}v_{\mathrm{PCC}_i}^{\alpha}i_{\mathrm{PCC}_i}^{\alpha} + \dfrac{1}{2}v_{\mathrm{PCC}_i}^{\beta}i_{\mathrm{PCC}_i}^{\beta}\\ Q_{\mathrm{PCC}_i} = \dfrac{1}{2}v_{\mathrm{PCC}_i}^{\beta}i_{\mathrm{PCC}_i}^{\alpha} - \dfrac{1}{2}v_{\mathrm{PCC}_i}^{\alpha}i_{\mathrm{PCC}_i}^{\beta}\end{cases} \tag{12}$$

In addition,

$$\begin{cases} \nabla P_{\mathrm{PCC}_i} = \dfrac{1}{2}v_{\mathrm{PCC}_i}^{\alpha}\dfrac{di_{\mathrm{PCC}_i}^{\alpha}}{dt} + \dfrac{1}{2}i_{\mathrm{PCC}_i}^{\alpha}\dfrac{dv_{\mathrm{PCC}_i}^{\alpha}}{dt}\\ \qquad + \dfrac{1}{2}v_{\mathrm{PCC}_i}^{\beta}\dfrac{di_{\mathrm{PCC}_i}^{\beta}}{dt} + \dfrac{1}{2}i_{\mathrm{PCC}_i}^{\beta}\dfrac{dv_{\mathrm{PCC}_i}^{\alpha}}{dt}\\ \nabla Q_{\mathrm{PCC}_i} = \dfrac{1}{2}v_{\mathrm{PCC}_i}^{\beta}\dfrac{di_{\mathrm{PCC}_i}^{\alpha}}{dt} + \dfrac{1}{2}i_{\mathrm{PCC}_i}^{\alpha}\dfrac{dv_{\mathrm{PCC}_i}^{\beta}}{dt}\\ \qquad - \dfrac{1}{2}v_{\mathrm{PCC}_i}^{\alpha}\dfrac{di_{\mathrm{PCC}_i}^{\beta}}{dt} - \dfrac{1}{2}i_{\mathrm{PCC}_i}^{\beta}\dfrac{dv_{\mathrm{PCC}_i}^{\alpha}}{dt}\end{cases} \tag{13}$$

where $\nabla P_{\mathrm{PCC}_i}$ and $\nabla Q_{\mathrm{PCC}_i}$ are the gradients of active and reactive power at the i^{th} local PCC, respectively.

$$\begin{cases} \dfrac{dv_{\mathrm{PCC}_i}^{\alpha}}{dt} = -\omega v_{\mathrm{PCC}_i}^{\beta}\\ \dfrac{di_{\mathrm{PCC}_i}^{\alpha}}{dt} = \dfrac{\omega v_{\mathrm{PCC}_i}^{\alpha}}{X_{\mathrm{TH}_i}} - \dfrac{\omega v_{\mathrm{TH}_i}^{\alpha}}{X_{\mathrm{TH}_i}} - \dfrac{\omega R_{\mathrm{TH}_i}i_{\mathrm{PCC}_i}^{\alpha}}{X_{\mathrm{TH}_i}}\\ \dfrac{dv_{\mathrm{PCC}_i}^{\beta}}{dt} = \omega v_{\mathrm{PCC}_i}^{\alpha}\\ \dfrac{di_{\mathrm{PCC}_i}^{\beta}}{dt} = \dfrac{\omega v_{\mathrm{PCC}_i}^{\beta}}{X_{\mathrm{TH}_i}} - \dfrac{\omega v_{\mathrm{TH}_i}^{\beta}}{X_{\mathrm{TH}_i}} - \dfrac{\omega R_{\mathrm{TH}_i}i_{\mathrm{PCC}_i}^{\beta}}{X_{\mathrm{TH}_i}}\end{cases} \tag{14}$$

where ω is the angular frequency of power grids.

Taking (14) into account, (13) can be rewritten as follows:

$$\begin{cases} \nabla P_{\mathrm{PCC}_i} = -\omega\Bigg(\dfrac{R_{\mathrm{TH}_i}P_{\mathrm{PCC}_i}}{X_{\mathrm{TH}_i}} + Q_{\mathrm{PCC}_i} - \dfrac{|v_{\mathrm{PCC}_i}^{\alpha} + v_{\mathrm{PCC}_i}^{\beta}|^2}{2X_{\mathrm{TH}_i}}\\ \qquad + \left(\dfrac{2v_{\mathrm{PCC}_i}^{\alpha}v_{\mathrm{PCC}_i}^{\beta} + v_{\mathrm{PCC}_i}^{\alpha}v_{\mathrm{TH}_i}^{\alpha} + v_{\mathrm{PCC}_i}^{\beta}v_{\mathrm{TH}_i}^{\beta}}{2X_{\mathrm{TH}_i}}\right)\Bigg)\\ \nabla Q_{\mathrm{PCC}_i} = \omega\Bigg(P_{\mathrm{PCC}_i} - \dfrac{R_{\mathrm{TH}_i}Q_{\mathrm{PCC}_i}}{X_{\mathrm{TH}_i}}\\ \qquad + \dfrac{v_{\mathrm{PCC}_i}^{\alpha}v_{\mathrm{TH}_i}^{\beta} - v_{\mathrm{PCC}_i}^{\beta}v_{\mathrm{TH}_i}^{\alpha}}{2X_{\mathrm{TH}_i}}\Bigg)\end{cases} \tag{15}$$

Equation (15) real-time solutions for $v_{\mathrm{TH}_i}^{\alpha}$ and $v_{\mathrm{TH}_i}^{\beta}$, which contains the information related to real-time variations in active and reactive power set-points at nearby PCCs. In particular, $v_{\mathrm{TH}_i}^{\alpha}$ and $v_{\mathrm{TH}_i}^{\beta}$ are determined as follows:

$$\begin{cases} v_{\mathrm{TH}_i}^{\alpha} = \dfrac{-1}{||V_{\mathrm{PCC}_i}||_2^2}\Bigg[v_{\mathrm{PCC}_i}^{\alpha}\left(\frac{2X_{\mathrm{TH}_i}\nabla P_{\mathrm{PCC}_i}}{\omega} + 2R_{\mathrm{TH}_i}P_{\mathrm{PCC}_i}\right.\\ \qquad \left. + 2X_{\mathrm{TH}_i}Q_{\mathrm{PCC}_i} - ||V_{\mathrm{PCC}_i}||_2^2\right)\\ \qquad + v_{\mathrm{PCC}_i}^{\beta}\left(\frac{2X_{\mathrm{TH}_i}\nabla Q_{\mathrm{PCC}_i}}{\omega} - 2X_{\mathrm{TH}_i}P_{\mathrm{PCC}_i}\right.\\ \qquad \left. + 2R_{\mathrm{TH}_i}P_{\mathrm{PCC}_i}\right)\Bigg]\\ v_{\mathrm{TH}_i}^{\beta} = \dfrac{-1}{||V_{\mathrm{PCC}_i}||_2^2}\Bigg[v_{\mathrm{PCC}_i}^{\beta}\left(\frac{2X_{\mathrm{TH}_i}\nabla P_{\mathrm{PCC}_i}}{\omega} + 2R_{\mathrm{TH}_i}P_{\mathrm{PCC}_i}\right.\\ \qquad \left. + 2X_{\mathrm{TH}_i}Q_{\mathrm{PCC}_i} - ||V_{\mathrm{PCC}_i}||_2^2\right)\\ \qquad - v_{\mathrm{PCC}_i}^{\alpha}\left(\frac{2X_{\mathrm{TH}_i}\nabla Q_{\mathrm{PCC}_i}}{\omega} - 2X_{\mathrm{TH}_i}P_{\mathrm{PCC}_i}\right.\\ \qquad \left. + 2R_{\mathrm{TH}_i}P_{\mathrm{PCC}_i}\right)\Bigg]\end{cases} \tag{16}$$

where $||V_{\mathrm{PCC}_i}||_2^2 = |v_{\mathrm{PCC}_i}^{\alpha} + v_{\mathrm{PCC}_i}^{\beta}|^2 - 2v_{\mathrm{PCC}_i}^{\alpha}v_{\mathrm{PCC}_i}^{\beta}$.

Algorithm 1: Pseudocode for the Proposed PIDMS.

```
Inputs: $P_{\text{ref}_i}^{\text{cyber}}$, $Q_{\text{ref}_i}^{\text{cyber}}$, $\kappa_i$, RST, $P_{\text{PV}_i}^{\max}$, $P_{\text{PV}_i}^{\min}$, $Q_{\text{inv}_i}^{\max}$, and $Q_{\text{inv}_i}^{\min}$
Outputs: $P^*$, $Q^*$, and INT
if $P_{\text{ref}_i}^{\text{cyber}} > P_{\text{PV}_i}^{\max}$ or $P_{\text{ref}_i}^{\text{cyber}} < P_{\text{PV}_i}^{\min}$ or $Q_{\text{ref}_i}^{\text{cyber}} > Q_{\text{inv}_i}^{\max}$ or $Q_{\text{ref}_i}^{\text{cyber}} < Q_{\text{inv}_i}^{\min}$ then
    INT = HIGH
else if $\kappa_i < 0$ then
    INT = HIGH
else
    INT = LOW
end if
if RST == 1 then
    INT = LOW
end if
if INT == HIGH then
    $P^* = 1.5$ kW, $Q^* = 0$ kVAR
else
    $P^* = P_{\text{ref}_i}^{\text{cyber}}$, $Q^* = Q_{\text{ref}_i}^{\text{cyber}}$
end if
```

Considering (16), the voltage magnitude and voltage phase angle at the i^{th} local PCC can be constructed, as follows:

$$\begin{cases} \left|\left|V_{\text{TH}_i}\right|\right|_2 = \sqrt{\left|v_{\text{TH}_i}^{\alpha} + v_{\text{TH}_i}^{\beta}\right|^2 - 2v_{\text{TH}_i}^{\alpha} v_{\text{TH}_i}^{\beta}} \\ \delta_{\text{TH}_i} = \tan^{-1}\left(\frac{v_{\text{TH}_i}^{\beta}}{v_{\text{TH}_i}^{\alpha}}\right) - \omega t \end{cases} \quad (17)$$

Algorithm 1 shows the operation of the proposed PIDMS. Particularly, the proposed PIDMS continuously checks and verifies if the newly commanded active and reactive power set-points, i.e., $P_{\text{ref}_i}^{\text{cyber}}$ and $Q_{\text{ref}_i}^{\text{cyber}}$, are within the operating limits of the grid-connected PV system. According to Fig. 1, the cyber intruder may attempt to only manipulate the operating set-points $(P_{\text{ref}_1}^{\text{cyber}}, Q_{\text{ref}_1}^{\text{cyber}})$. This means that the cyber intruder has no access to the measured data. In this regard, the cyber intrusion can be modeled as follows:

$$\begin{bmatrix} P_{\text{ref}_1}^{\text{cyber}} \\ Q_{\text{ref}_1}^{\text{cyber}} \end{bmatrix} = \begin{bmatrix} P_{\text{ref}_1}^{\text{cyber,T}} \\ Q_{\text{ref}_1}^{\text{cyber,T}} \end{bmatrix} + \begin{bmatrix} P_{\text{ref}_1}^{\text{cyber,A}} \\ Q_{\text{ref}_1}^{\text{cyber,A}} \end{bmatrix} \quad (18)$$

where $P_{\text{ref}_1}^{\text{cyber,T}}$ and $Q_{\text{ref}_1}^{\text{cyber,T}}$ are the true commanded active and reactive power set-points, respectively, and $P_{\text{ref}_1}^{\text{cyber,A}}$ and $Q_{\text{ref}_1}^{\text{cyber,A}}$ are the injected active and reactive power set-points by the cyber intruder, respectively.

If the new active and reactive power set-points are respectively greater than the maximum operating limits of the PV array $(P_{\text{PV}_i}^{\max})$ and the DC/AC inverter $(Q_{\text{inv}_i}^{\max})$ or less than their minimum operating limits, i.e., $P_{\text{PV}_i}^{\min}$ and $Q_{\text{inv}_i}^{\min}$, the INT flag is raised to **HIGH**. Otherwise, the INT flag is **LOW**, indicating the normal operation of the grid-connected PV system. In addition, the stability index (κ_i) is being dynamically checked, and the normal operation of the system is guaranteed if $\kappa_i > 0$. Otherwise, the abnormal behavior of the system is detected when $\kappa_i < 0$, and accordingly, the INT flag is raised to **HIGH**. In order for the power systems operator to manually reset the status of the cyber layer once the necessary actions have been taken, an RST signal is incorporated into the Algorithm. In this regard, if the RST signal is 1, the INT flag changes to **LOW**, reverting the status of the cyber layer to the normal operating condition. Once the operating limits, as well as the stability index, are checked, and the commanded active and reactive power set-points are flagged as compromised set-points by raising the INT flag to **HIGH**, the proposed PIDMS adjusts the commanded active and reactive power set-points such that the new operating set-points belong to the normal operating region, i.e., $P^* = 1.5$ kW and $Q^* = 0$ kVAR, where P^* and Q^* denote the active and reactive power set-points sent to the control layer. Otherwise, when the INT flag is **LOW**, the commanded active and reactive power set-points received by the cyber layer are assigned to the control layer without further changes, i.e., $P^* = P_{\text{ref}_i}^{\text{cyber}}$ and $Q^* = Q_{\text{ref}_i}^{\text{cyber}}$.

According to Fig. 1, the physical layer comprises a two-stage transformerless grid-connected PV system with DC/DC and DC/AC conversion stages. Figs. 2 and 3 show the structures of the cyber layer with the proposed PIDMS and the control layer for a grid-connected PV system, respectively. In this regard, $P_{\text{ref}_i}^{\text{cyber}}$ and $Q_{\text{ref}_i}^{\text{cyber}}$ are sent to the cyber layer, and after further processes, the operating active and reactive power set-points of the i^{th} local PCC are assigned by the cyber layer to the control layer. The injected active power into the DC-link from the PV array is regulated by controlling the duty cycle (D) of the DC/DC power converter at a specified DC-link voltage level. In particular, the DC/DC power converter controls the i^{th} PV array voltage (v_{PV_i}), thus, controlling the operating set-point and determining the injected power by the PV array. The DC/AC inverter regulates both the DC-link voltage and the reactive power injected into power grids by controlling the modulation index (M). Using a Phase Locked Loop (PLL) and the Park transformation, the DC/AC inverter regulates the DC-link voltage by controlling the d-axis current at the i^{th} local PCC (I_d) and the injected reactive power into power grids by controlling the q-axis current at the i^{th} local PCC (I_q) [31]. In Fig. 3, L_{inv_i} denotes the total inductance of the filter inductors connected to the grid-connected PV inverter output on a per-unit basis.

III. Results and Discussion

The theoretical analyses established are validated by dynamic simulation of four scenarios. The specifications of the case study for the $i = 1^{\text{st}}$ grid-connected PV system are provided in Table I. In the first three seconds of the simulation (from $t = 0$ s to $t = 3$ s), the DC/DC power converter operates at a constant duty cycle, and the control system is disregarded. During this time interval, the initial $Q_{\text{ref}_1}^{\text{cyber}}$ and the DC-link voltage reference $(v_{\text{DC}_1}^*)$ are set to 0 kVAR and 1 kV (nominal kV-rating), respectively.

Case Study I

Fig. 4 shows the power generated by the PV array (P_{PV_1}) and the active power (P_{PCC_1}) and reactive power (Q_{PCC_1}) injected into power grids at the first local PCC. In addition, Fig. 5 illustrates the active power–reactive power–voltage contours for the PV inverter at the first local PCC. According to Fig. 4, the PV array generates approximately 2 kW of power, and once the DC-link voltage reaches its reference value, i.e., 1 kV, neglecting power

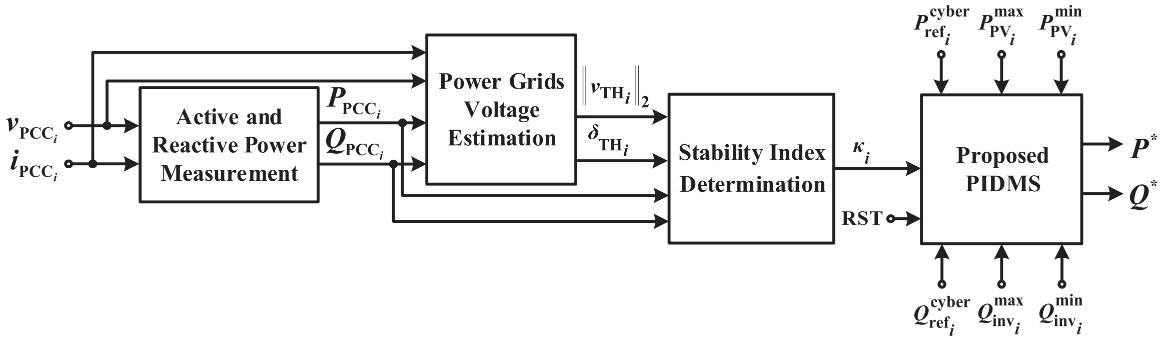

v_{PCC_i}
i_{PCC_i}
Active and Reactive Power Measurement
P_{PCC_i}
Q_{PCC_i}
Power Grids Voltage Estimation
$\|v_{\mathrm{TH}_i}\|_2$
δ_{TH_i}
Stability Index Determination
κ_i
RST
$P_{\mathrm{ref}_i}^{\mathrm{cyber}}$
$P_{\mathrm{PV}_i}^{\mathrm{max}}$
$P_{\mathrm{PV}_i}^{\mathrm{min}}$
Proposed PIDMS
P^*
Q^*
$Q_{\mathrm{ref}_i}^{\mathrm{cyber}}$
$Q_{\mathrm{inv}_i}^{\mathrm{max}}$
$Q_{\mathrm{inv}_i}^{\mathrm{min}}$

Fig. 2. Structure of the cyber layer with the proposed PIDMS for a grid-connected PV system.

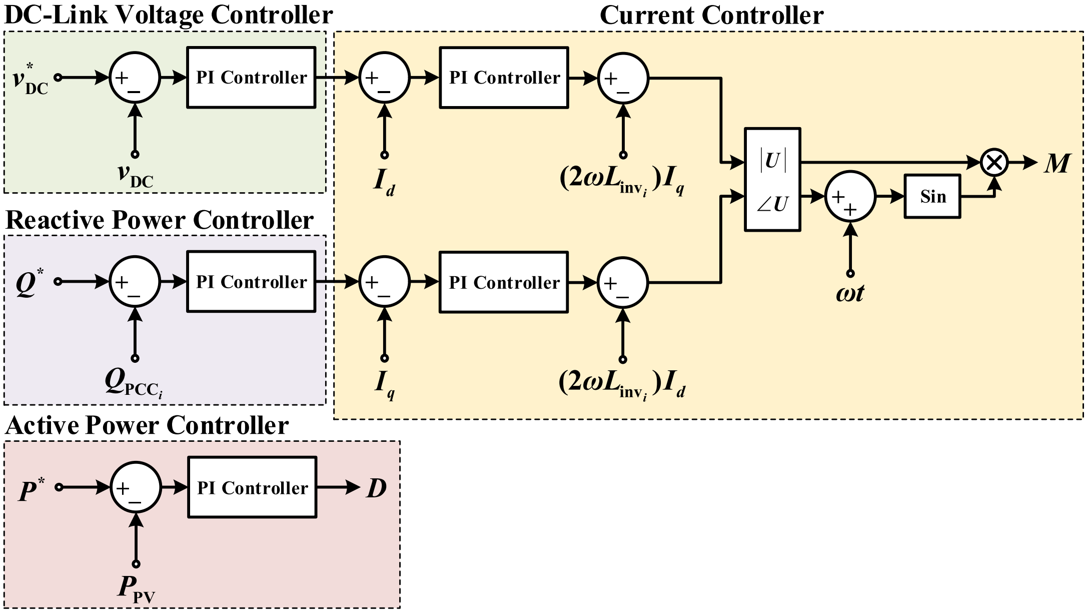


Fig. 3. Structure of the control layer for a grid-connected PV system.

TABLE I
SPECIFICATIONS OF THE FIRST GRID-CONNECTED PV SYSTEM

Parameters	Values
PV Inverter Rated Power ($S_{\mathrm{PV}_1}^{\mathrm{rated}}$)	2.5 kVA
Switching Frequency (f_{sw})	10 kHz
Nominal Power Grids Frequency (f)	60 Hz
Nominal Power Grids Voltage (V_{TH_1})	120 V
Nominal DC-Link Voltage (v_{DC_1})	1 kV
DC-Link Capacitor (C_{DC_1})	3000 μF
Filter Inductors (L_{1,inv_1} and L_{2,inv_1})	17.4 mH and 55 μH
Filter Capacitor (C_{inv_1})	27.5 μF
PV Array Capacitor (C_{PV_1})	1000 μF
DC/DC Converter Inductor (L_{con})	5 mH
Thévenin Equivalent Resistance (R_{TH_1})	15 Ω
Thévenin Equivalent Inductance (L_{TH_1})	100 μH

losses, the same amount of power is injected into power grids to maintain the DC-link voltage constant, as shown in Fig. 6. Fig. 7(a) and 7(b) illustrate the voltage and current at the first local PCC, respectively.

In the first scenario, from $t = 3$ s to $t = 8$ s, $P_{\mathrm{ref}_1}^{\mathrm{cyber}}$ is set to 2 kW, which is within the operating limits of the PV system, without additional changes in $Q_{\mathrm{ref}_1}^{\mathrm{cyber}}$, and it is considered that none of the operating set-points passed through the cyber layer are manipulated. Therefore, as shown in Fig. 8, κ_1 is greater than zero, and the INT flag is **LOW**, indicating that the normal operation of the system is guaranteed. Accordingly, as shown in Fig. 5, $P^* = P_{\mathrm{ref}_1}^{\mathrm{cyber}} = 2\,\mathrm{kW}$ and $Q^* = Q_{\mathrm{ref}_1}^{\mathrm{cyber}} = 0\,\mathrm{kVAR}$, indicated by set-point **A**. As shown in Figs. 4 and 6, the generated power by the PV array is 2 kW, the injected power into power grids is ∼2 kW, and the DC-link voltage is fixed at 1 kV. According to Fig. 7(a) and 7(b), the peak values of the voltage and current at the first local PCC are 348.1 V and 11.9 A, respectively.

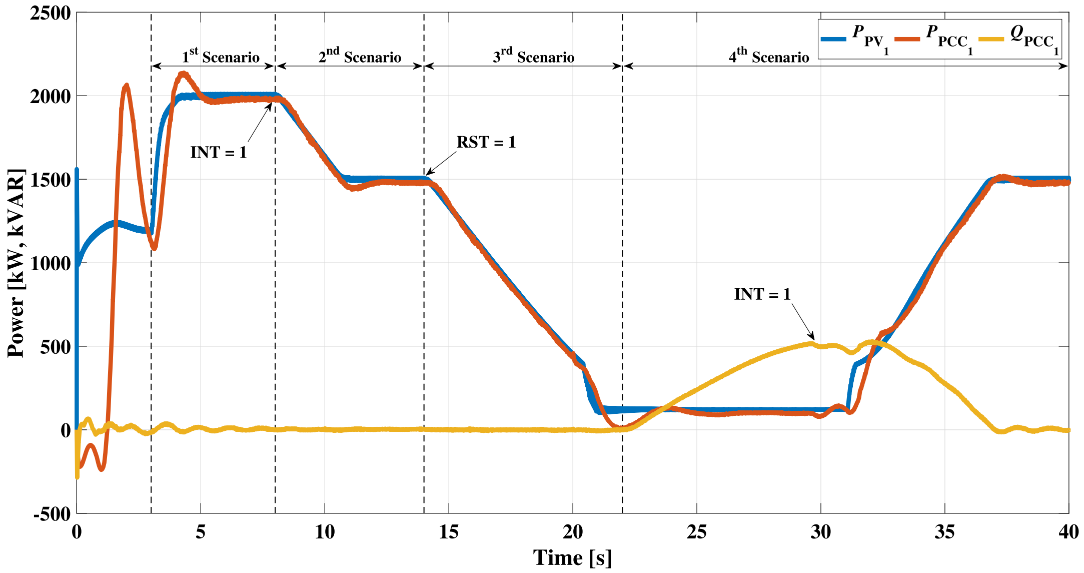


Fig. 4. Simulation results for the power generated by the PV array and the active power and reactive power injected into power grids at the first local PCC for Case Study I.

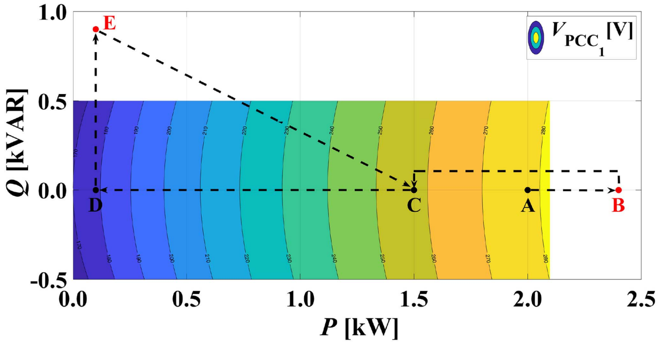


Fig. 5. Simulation results for the active power–reactive power–voltage contours for the PV inverter at the first local PCC for Case Study I.

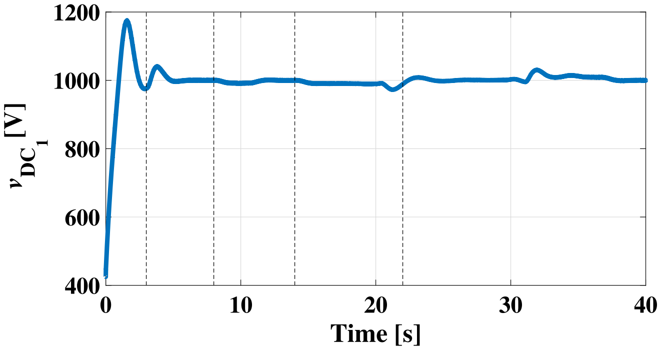
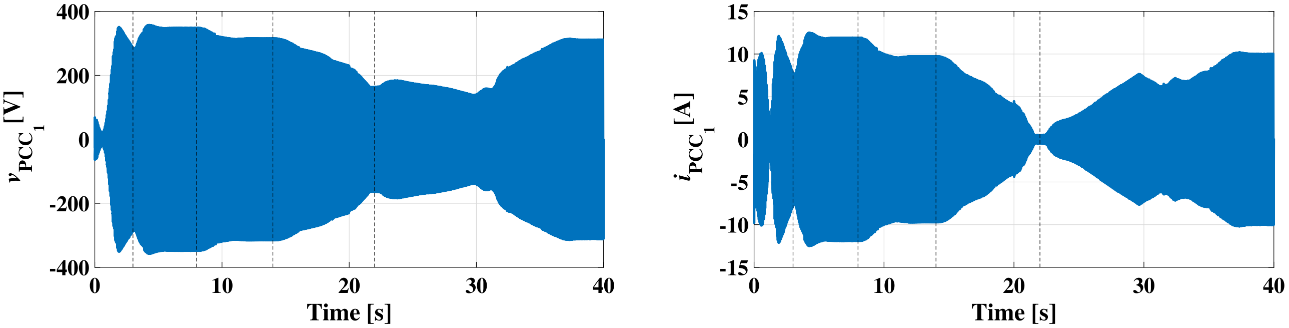


Fig. 6. Simuation results for the DC-link voltage of the PV inverter for Case Study I.

In the second scenario, at $t = 8$ s, $P^{\text{cyber}}_{\text{ref}_1}$ is manipulated and increased to 2.4 kW, which is greater than $P^{\max}_{\text{PV}_1}$. This is shown by set-point **B** in Fig. 5, which is outside the normal operating region. As shown in Fig. 8(a), the INT flag is raised to **HIGH**, and the proposed PIDMS pushes the active power and reactive power set-points to stable operating set-points, i.e., $P^* = 1.5$ kW and $Q^* = 0$ kVAR, as shown by set-point **C** in Fig. 5. In this regard, between $t = 8$ s and $t = 14$ s, κ_1 is still greater than zero. As demonstrated in Fig. 7(a) and 7(b), the reduction in the active power injected into power grids, and accordingly, the current injected into power grids, leads to a reduction in the peak values of voltage and current at the first local PCC to 313.9 V and 9.6 A, respectively.

In the third scenario, since the INT flag is already **HIGH**, at $t = 14$ s, the RST signal is activated, thus, resetting the INT flag and bringing the system to the normal operating condition, as shown in Fig. 8(c). Thereafter, as shown by set-point **D** in Fig. 5, $P^{\text{cyber}}_{\text{ref}_1}$ is set to 0.1 kW while $Q^{\text{cyber}}_{\text{ref}_1}$ remains unchanged. Based on Fig. 4, the generated power by the PV array reaches 0.1 kW at $t = 21$ s. From $t = 14$ s to $t = 22$ s, since the generated power by the PV array is decreasing, the DC-link voltage controller adjusts its output, and accordingly, the PV inverter injects less power into power grids. Fig. 9 shows the measured and estimated voltage of power grids. According to this figure, at $t = 20$ s, the power grids voltage decreases (v_{TH_1}), and since the estimated voltage ($v^{\text{est}}_{\text{TH}_1}$) follows the measured voltage of power grids, the performance of the power grids voltage estimation block can be verified.

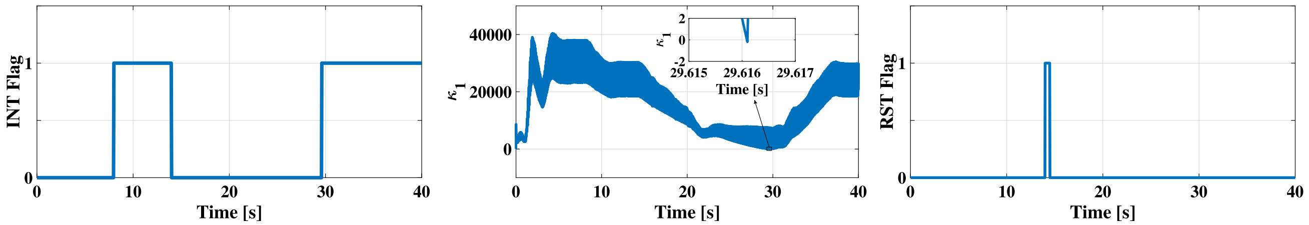
In the last scenario, which starts at $t = 22$ s, as illustrated by set-point **E** in Fig. 5, the $Q^{\text{cyber}}_{\text{ref}_1}$ is manipulated and changed to 0.9 kVAR. According to Fig. 8(b), by reaching the injected reactive power into power grids 0.515 kVAR, κ_1 becomes negative, and the INT flag is raised to **HIGH**, indicating that the PV system enters an unstable region. As a result, the proposed PIDMS ensures the stable operation of the PV system by pushing the active power and reactive power set-points to stable operating set-points, i.e., $P^* = 1.5$ kW and $Q^* = 0$ kVAR, as shown by set-point **C** in Fig. 5.



(a)

(b)

Fig. 7. Simulation results for the (a) voltage and (b) current at the first local PCC for Case Study I.



(a)

(b)

(c)

Fig. 8. Simulation results for the (a) intrusion flag, (b) stability index, and (c) reset signal for Case Study I.

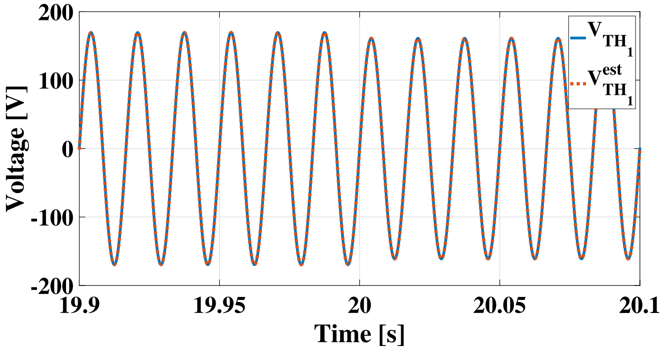


Fig. 9. Measured versus estimated voltage of power grids at the first local PCC for Case Study I.

Case Study II

Figs. 10 to 15 illustrate a new set of simulation results for further evaluating the performance of the proposed PIDMS. In the first scenario, from $t = 3$ s to $t = 8$ s, $P_{\mathrm{ref}_1}^{\mathrm{cyber}}$ is set to 1.2 kW, which is within the operating limits of the PV system, and $Q_{\mathrm{ref}_1}^{\mathrm{cyber}}$ is set to 0.2 kVAR. Fig. 10 shows that the active power and reactive power reached their predefined values, and none of the operating set-points passed through the cyber layer are manipulated. According to Fig. 14, since $\kappa_1 > 0$, the INT flag is **LOW**, and the normal operating conditions are guaranteed. Taking Fig. 11 into account, $P^* = P_{\mathrm{ref}_1}^{\mathrm{cyber}} = 1.2$ kW and $Q^* = Q_{\mathrm{ref}_1}^{\mathrm{cyber}} = 0.2$ kVAR, which indicate the set-point $\mathbf{A}'$. Figs. 10 and 12 confirm that the generated power by the PV array is 1.2 kW, the injected power into power grids is ~1.2 kW, and the DC-link voltage is fixed at 1 kV. As shown in Fig. 13, the peak values of the voltage and current at the first local PCC are 292.3 V and 8.39 A, respectively.

The second scenario is similar to the first one with slight changes in the PV array set-points, i.e., $P^* = P_{\mathrm{ref}_1}^{\mathrm{cyber}} = 0.9$ kW and $Q^* = Q_{\mathrm{ref}_1}^{\mathrm{cyber}} = 0.4$ kVAR, shown by set-point $\mathbf{B}'$ in Fig. 11. The simulation results confirm that the desired outputs are achieved.

In the third scenario, at $t = 18$ s, both $P_{\mathrm{ref}_1}^{\mathrm{cyber}}$ and $Q_{\mathrm{ref}_1}^{\mathrm{cyber}}$ are manipulated and their corresponding values are increased by three times. Since the new set-points $P_{\mathrm{ref}_1}^{\mathrm{cyber}} = 2.7$ kW and $Q_{\mathrm{ref}_1}^{\mathrm{cyber}} = 1.2$ kVAR are respectively greater than $P_{\mathrm{PV}_1}^{\max}$ and $Q_{\mathrm{inv}_1}^{\max}$. This is shown by set-point $\mathbf{C}'$ in Fig. 11, which is not within the normal operating region. According to Fig. 14(a), the INT flag is raised to **HIGH**, and the proposed PIDMS pushes the active and reactive power set-points to stable operating set-points, i.e., $P^* = 1.5$ kW and $Q^* = 0$ kVAR, as shown by set-point $\mathbf{D}'$, which is similar to set-point **C** in Fig. 5. Thus, between $t = 18$ s and $t = 25$ s, κ_1 is still greater than zero.

In the fourth scenario, due to the fact that the INT flag is already **HIGH**, at $t = 25$ s, the RST signal is activated, and therefore, the INT flag is reset, and the system is brought to the normal operating conditions, as shown in Fig. 14(c). After that, $P_{\mathrm{ref}_1}^{\mathrm{cyber}}$ and $Q_{\mathrm{ref}_1}^{\mathrm{cyber}}$ are set to 1.2 kW and 0.4 kVAR, respectively, as shown by set-point $\mathbf{E}'$ in Fig. 11. According to Fig. 10, at $t = 28$ s, the generated power by the PV array and the injected reactive power into power grids reach 1.2 kW and 0.4 kVAR, respectively. Additionally, at $t = 30$ s, the power grids voltage increased by 15%, as shown in Fig. 15. The estimated voltage follows the measured voltage of power grids, which in turn,

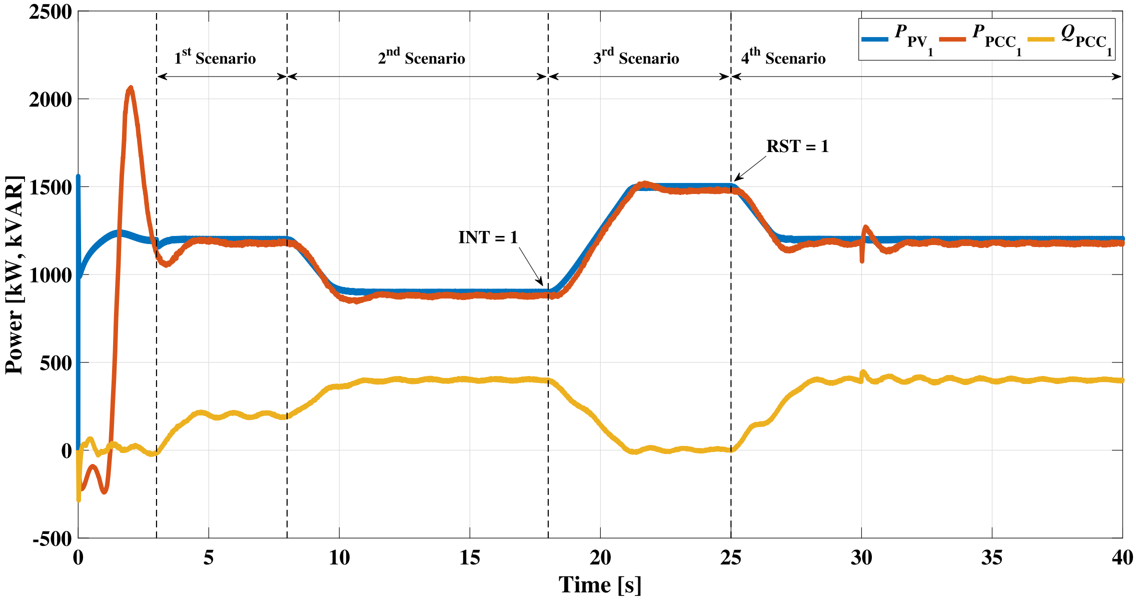


Fig. 10. Simulation results for the power generated by the PV array and the active power and reactive power injected into power grids at the first local PCC for Case Study II.

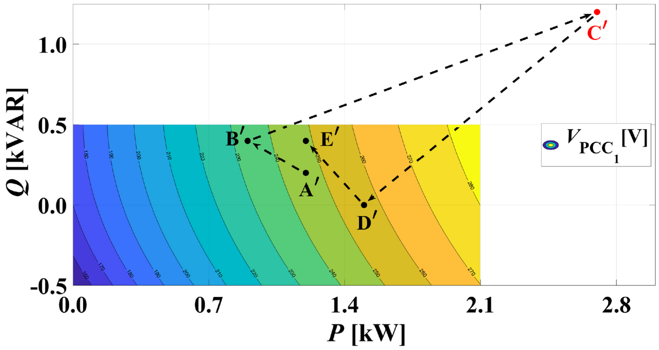


Fig. 11. Simulation results for the active power–reactive power–voltage contours for the PV inverter at the first local PCC for Case Study II.

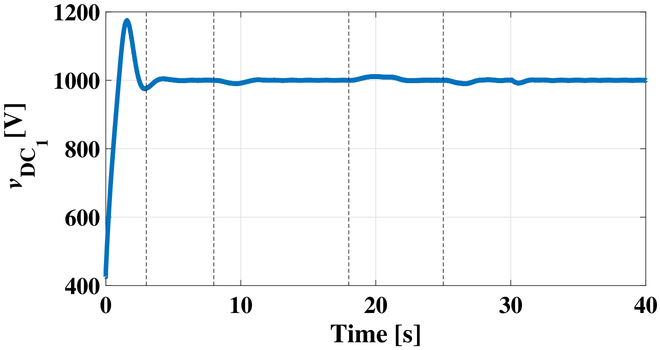
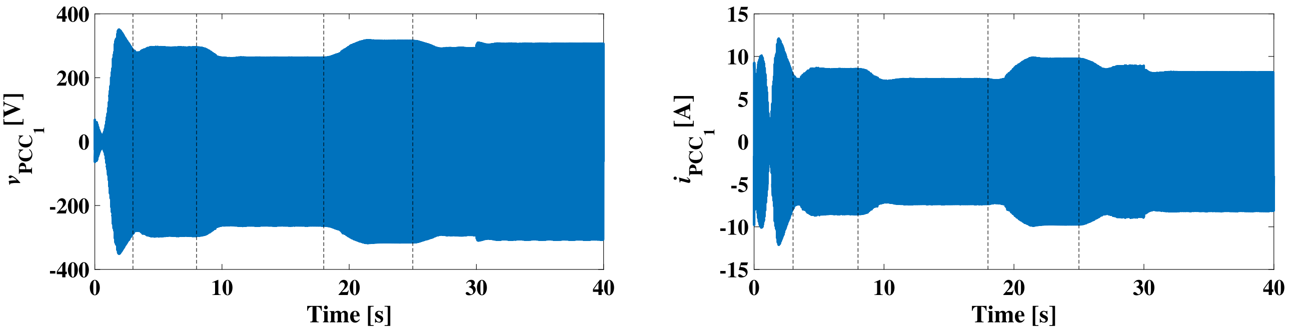


Fig. 12. Simulation results for the DC-link voltage of the PV inverter for Case Study II.

verifies the performance of the power grids voltage estimation block.

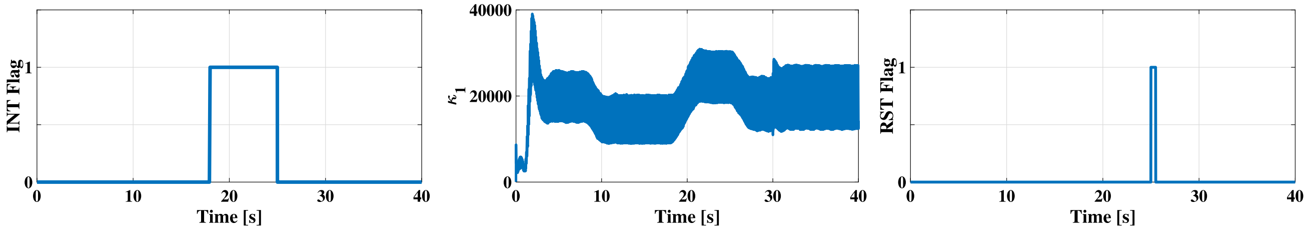
Case Study III

Fig. 16 demonstrates the simulation results for evaluating the performance of the proposed PIDMS when the solar irradiance level and solar cell temperature vary and the commanded $P_{\text{ref}_1}^{\text{cyber}}$ and $Q_{\text{ref}_1}^{\text{cyber}}$ are set to 1.0 kW and 0.0 kVAR, respectively. From $t = 0$ s to $t = 6$ s, the initial solar irradiance and solar cell temperature are set to 1000 W/m ^{2} and 25 °C, respectively. Based on Fig. 16(a), the power generated by the PV array (P_{PV_1}) and the active power (P_{PCC_1}) and reactive power (Q_{PCC_1}) injected into power grids at the first local PCC reach 1.0 kW and 0 kVAR, respectively. As shown in Fig. 16(b), particularity between $t = 3$ s and $t = 6$ s, the PV array voltage and current are 166.4 V and 6.02 A, respectively. At $t = 6$ s, the solar irradiance decreases by 200 W/m ^{2} and remains at the same level till $t = 25$ s with no additional changes in the solar cell temperature. During this time period, the PV array voltage and current are changed from 166.4 V to 209.4 V and 6.02 A to 4.79 A, respectively. At $t = 15$ s, the solar cell temperature decreases by 5 °C and remains constant for 10 s, i.e., till $t = 25$ s. According to Fig. 16(b), due to the reduction in the PV current level by decreasing the solar cell temperature, the control system increases the level of the PV array voltage from 207.9 V to 215.1 V to maintain the PV array active power at 1 kW. From $t = 25$ s to $t = 35$ s, the solar irradiance increases by 200 W/m ^{2} and reaches its initial value of 1000 W/m^2 with no changes in the solar cell temperature. As shown in Fig. 16(b), during this time period, the PV array voltage changes from 215.1 V to 170.4 V, and the PV current changes from 4.67 A to 5.87 A. Finally, at $t = 35$ s, the solar cell temperature increases by 5 °C and reaches 25 °C while the solar irradiance is 1000 W/m^2. Between $t = 35$ s and $t = 40$ s, the control system adjusts the level of the PV array voltage to maintain the PV array active power at 1 kW.



(a) (b)

Fig. 13. Simulation results for the (a) voltage and (b) current at the first local PCC for Case Study II.



(a) (b) (c)

Fig. 14. Simulation results for the (a) intrusion flag, (b) stability index, and (c) reset signal for Case Study II.

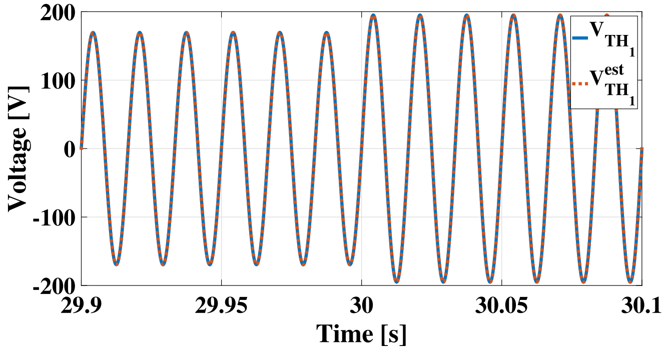


Fig. 15. Measured versus estimated voltage of power grids at the first local PCC for Case Study II.

TABLE II
SPECIFICATIONS OF THE FIRST GRID-CONNECTED PV SYSTEM FOR CASE STUDY IV

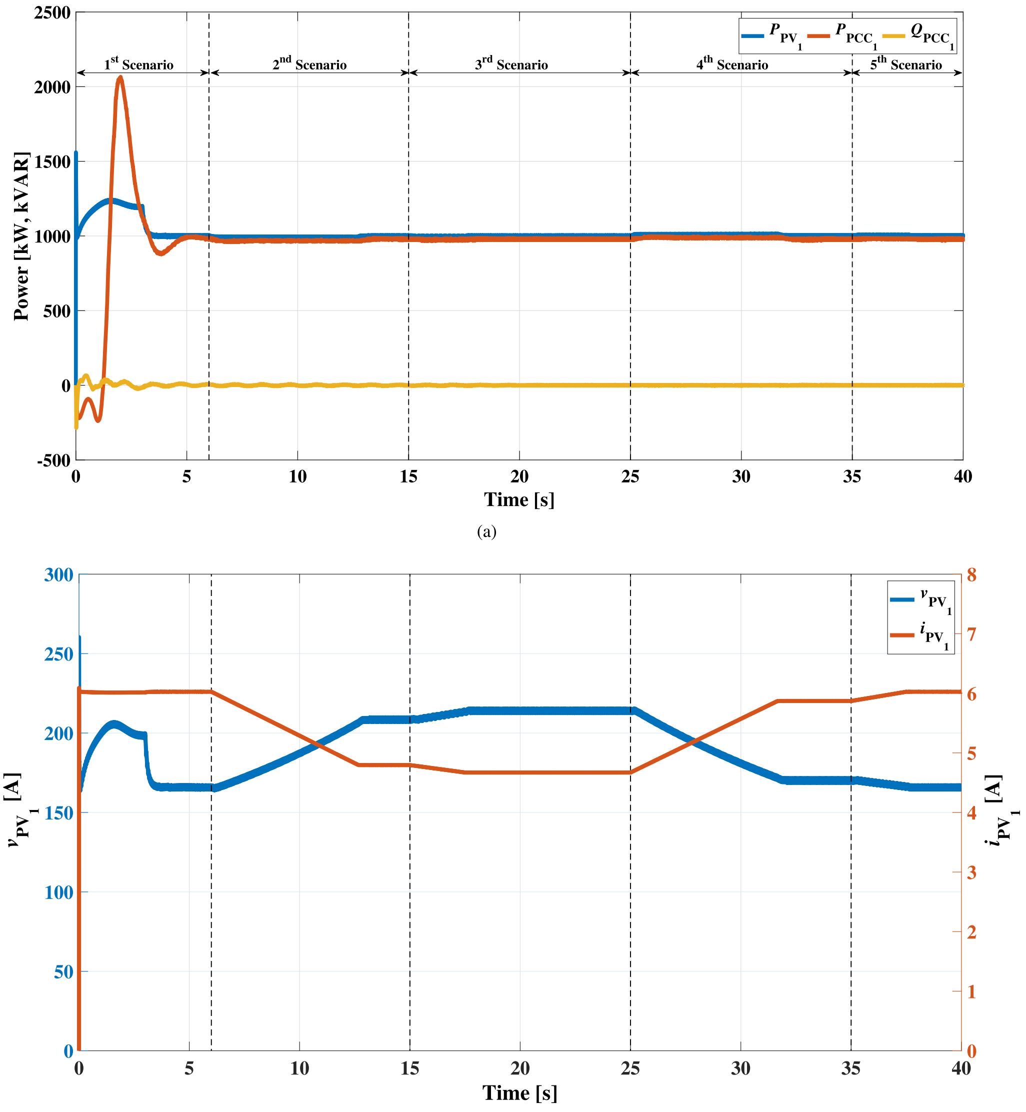
Parameters	Values
DC-Link Capacitor	2000 μF
Filter Inductors (L_{1,inv_1} and L_{2,inv_1})	10 mH and 55 μH
PV Array Capacitor (C_{PV_1})	600 μF
DC/DC Converter Inductor (L_{con})	4 mH
Thévenin Equivalent Inductance (L_{TH_1})	10 mH

Based on the obtained results, it can be observed that as long as the commanded $P_{\text{ref}_1}^{\text{cyber}}$ and $Q_{\text{ref}_1}^{\text{cyber}}$ are within the operating limits of the grid-connected PV system, the system can be properly operated under different solar irradiance levels and temperatures.

Case Study IV

Additionally, to ensure that the integration of the grid-connected PV system equipped with the proposed PIDMS does not disrupt normal operating conditions and changes in the parameters of the grid-connected PV system do not affect its performance, a new set of simulation results are provided where the changes are shown in Table II. Figs. 17 to 22 show the simulation results for evaluating the performance of the proposed PIDMS when the parameters of the grid-connected PV system change.

The same scenarios as Case Study I are considered for Case Study IV. In the first scenario, from $t = 3$ s to $t = 8$ s, $P_{\text{ref}_1}^{\text{cyber}} = 2$ kW and $Q_{\text{ref}_1}^{\text{cyber}} = 0$, which are both within the operating limits of the grid-connected PV system and no transmitted data manipulation occurs. According to Fig. 21, $\kappa_1 > 0$, and the INT flag is **LOW**, which ensures the normal operation of the grid-connected PV system. As illustrated in Fig. 18, $P^* = P_{\text{ref}_1}^{\text{cyber}} = 2$ kW and $Q^* = Q_{\text{ref}_1}^{\text{cyber}} = 0$ kVAR, indicated by set-point **A**$''$. Based on the results shown in Figs. 17, 19, and 20, (1) the generated power by the PV array is 2 kW, (2) the injected power into power grids is ~2 kW, (3) the DC-link voltage is fixed at 1 kV, and (4) the peak values of the voltage and current at the first local PCC are 348.1 V and 11.9 A, respectively. Compared to the first scenario in Case Study I, a smoother transient response with a 39% reduction in the overshoot of the active power injected into power grids at the first local PCC and reactive power oscillations



(a)

(b)

Fig. 16. Simulation results for (a) the power generated by the PV array and the active power and reactive power injected into power grids and (b) the PV array voltage and current at the first local PCC for Case Study III.

between 5% and 25% are observed. In addition, due to the reduction in the size of the DC-link capacitor, the DC voltage ripples are slightly increased. As shown in Figs. 17 and 21, by manipulating $P_{\mathrm{ref}_1}^{\mathrm{cyber}}$ at $t = 8$ s and increasing it to 2.4 kW (set-point $\mathbf{B}''$ in Fig. 18), $P_{\mathrm{PV}_1}^{\max}$ exceeds the maximum operating limits of the PV array, and accordingly, the INT flag is raised to **HIGH**. Therefore, the proposed PIDMS adjusts the active power and reactive power set-points to $P^* = 1.5$ kW and $Q^* = 0$ kVAR with $\kappa_1 > 0$, as illustrated by set-point $\mathbf{C}''$ in Fig. 18.

According to Fig. 20(a) and 20(b), when the active power injected into power grids decreases, the peak values of voltage and current at the first local PCC proportionally decrease. Compared to the second scenario in Case Study I, an improvement in the transient response of the active power injected into power grids at the first local PCC can be observed in Case Study IV. In the third scenario, as shown in Fig. 21, the INT flag is reset at $t = 14$ s by activating the RST signal at that time. According to Fig. 18, set-point $\mathbf{D}''$= ($P_{\mathrm{ref}_1}^{\mathrm{cyber}} = 0.1$ kW, $Q_{\mathrm{ref}_1}^{\mathrm{cyber}} = 0$ kVAR) is considered for the grid-connected PV system. As shown in Fig. 17, the generated power by the PV array reaches 0.1 kW at $t = 21.5$ s. Between $t = 14$ s and $t = 22$ s, the PV inverter injects less power into power grids due to the reduction in generated power by the PV array. Fig. 22 demonstrates the measured and estimated voltage of power grids. As shown in this figure, at $t = 20$ s, a reduction in the power grids voltage (v_{TH_1}) can be observed, and as the estimated voltage ($v_{\mathrm{TH}_1}^{\mathrm{est}}$) follows the measured voltage of power grids, the performance of the power grids voltage estimation block can be verified. The last scenario starts at $t = 22$ s, shown by set-point $\mathbf{E}''$ in Fig. 18, where $Q_{\mathrm{ref}_1}^{\mathrm{cyber}}$ is manipulated and changed to 0.9 kVAR. According to Fig. 17, at $t = 29.1$ s, when the injected reactive power into power grids reaches 0.595 kVAR, $\kappa_1 < 0$, and the INT flag is raised to **HIGH**. Therefore, the proposed PIDMS pushes the active power and reactive power set-points to stable operating set-points, i.e., $P^* = 1.5$ kW and $Q^* = 0$ kVAR, as shown by set-point $\mathbf{C}''$ in Fig. 18. Compared to the last scenario in

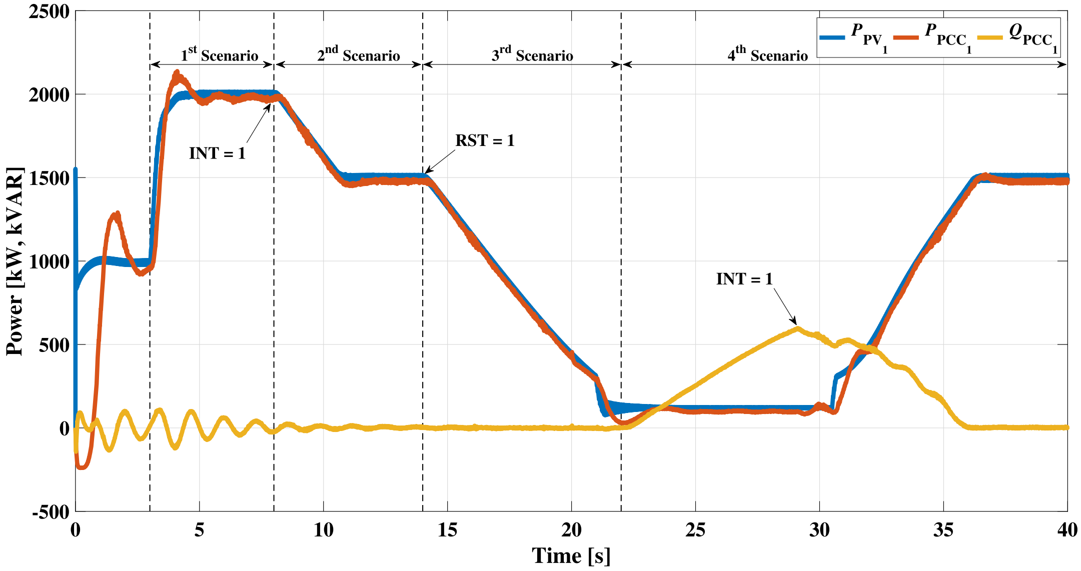


Fig. 17. Simulation results for the power generated by the PV array and the active power and reactive power injected into power grids at the first local PCC for Case Study IV.

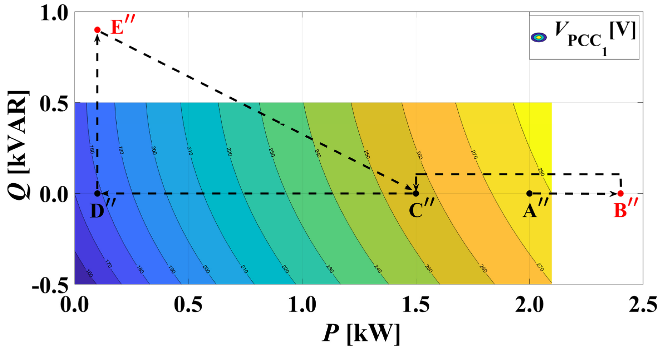


Fig. 18. Simulation results for the active power–reactive power–voltage contours for the PV inverter at the first local PCC for Case Study IV.

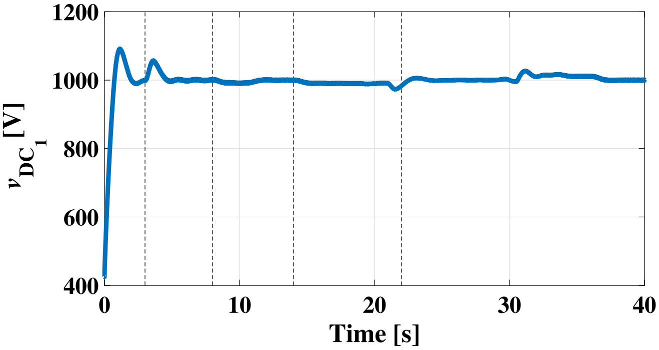


Fig. 19. Simulation results for the DC-link voltage of the PV inverter for Case Study IV.

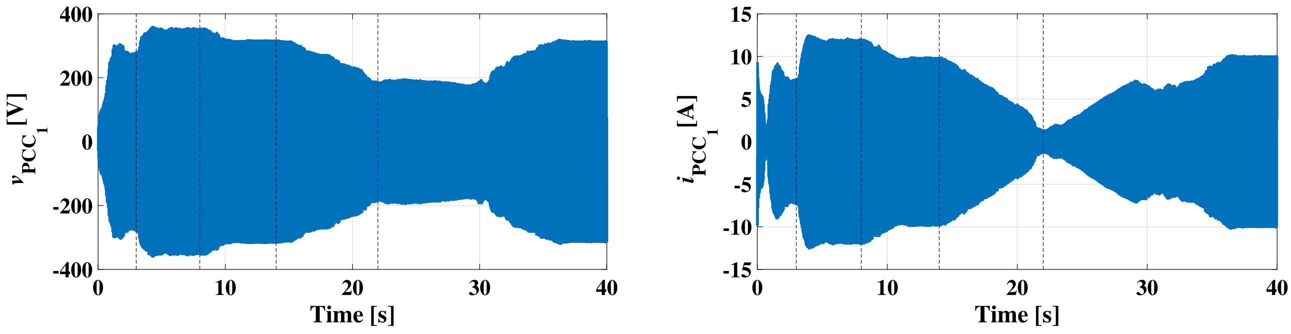
TABLE III
PERFORMANCE COMPARISON OF DIFFERENT DATA-DRIVEN ALGORITHMS WITH THE PROPOSED PIDMS FOR CASE STUDY I

Methods	Accuracy [%]
Logistic Regression (LR)	89.0
Support Vector Machine (SVM)	94.1
k-Nearest Neighbors (kNN)	92.5
Gradient Boosting (GBT)	96.2
Random Forest (RF)	96.3
Multi-Layer Perceptron (MLP)	96.2
Proposed PIDMS	99.5

Case Study I, the cyber intrusion is detected earlier due to the fact that the fundamental components of the grid-connected PV systems have been resized, (particularly, 33%, 42%, 40%, and 20% reduction in the sizes of the DC-capacitor (C_{DC_1}), the filter inductor (L_{1,inv_1}), the PV array capacitor (C_{PV_1}), and the DC/DC converter inductor (L_{con}), respectively, and 9900% increase in the Thévenin equivalent inductance (L_{TH_1})), leading to quickly achieving a negative value for κ_1.

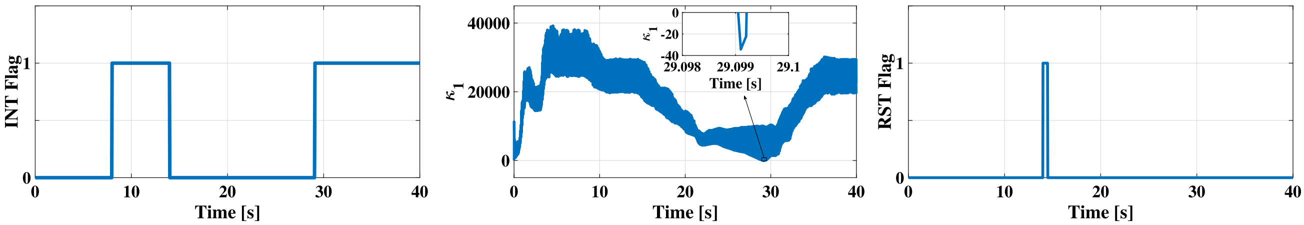
In order to compare the performance of the proposed PIDMS, different data-driven algorithms, such as Logistic Regression (LR), Support Vector Machine (SVM), k-Nearest Neighbors (kNN), Gradient Boosting (GBT), Random Forest (RF), and Multi-Layer Perceptron (MLP) with their corresponding optimal parameters have been analyzed. Table III shows a summary of the comparison of the mentioned data-driven algorithms with the proposed PIDMS for Case Study I. As shown in this table, the proposed PIDMS has a significantly higher accuracy compared to the other data-driven methods, while it does not require a training dataset.

In addition, Table IV shows the performance of the proposed PIDMS compared to several presented methods in the literature for Case Study I. Compared to the existing methods, the proposed method has a higher accuracy, and it is capable of detecting and mitigating cyber intrusions faster. It should be



(a) (b)

Fig. 20. Simulation results for the (a) voltage and (b) current at the first local PCC for Case Study IV.



(a) (b) (c)

Fig. 21. Simulation results for the (a) intrusion flag, (b) stability index, and (c) reset signal for Case Study IV.

TABLE IV
PERFORMANCE COMPARISON OF DIFFERENT METHODS IN THE LITERATURE WITH THE PROPOSED PIDMS FOR CASE STUDY I

Methods	Overall Accuracy [%]	Detection Time [s]	Training Data	Detection Capability	Mitigation Capability
[17]	95.3	NA	Required	✓	–
[22]	98.1	1.00	Required	✓	–
[32]	92.3	1.10	Not Required	✓	–
[33]	93.8	NA	Required	✓	–
[34]	96.5	NA	Required	✓	–
[35]	99.4	1.4	Required	✓	✓
Proposed PIDMS	99.5	0.21	Not Required	✓	✓

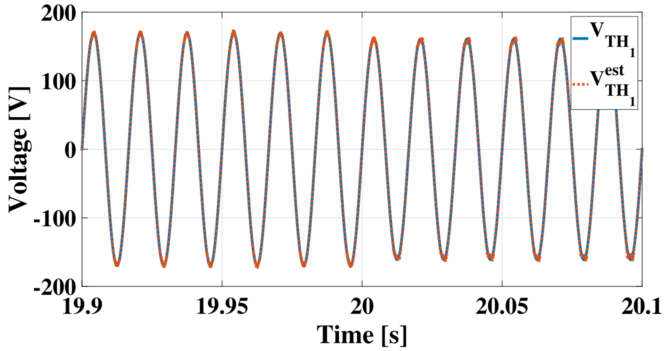


Fig. 22. Measured versus estimated voltage of power grids at the first local PCC for Case Study IV.

noted that the performance of the proposed PIDMS is dependent on the correct measurements of the voltage and current at its local PCC. Thus, if the measurements contain a high level of noise, or in the case of inaccurate measurements due to malfunctioning of the measurement devices, the performance of the proposed PIDMS may be affected. Furthermore, since the loadability of power grids has been determined using the Thévenin equivalent voltage and Thévenin series impedance, any drastic changes in such values may affect the performance of the proposed PIDMS.

IV. CONCLUSION

The main objective of this paper is to introduce a Proactive Intrusion Detection and Mitigation System (PIDMS) for a multi-layer controlled grid-connected Photovoltaic (PV) system to improve the situational awareness and observability and enhance the resilience of Cyber-Physical Power and Energy Systems (CPPES) against malicious False Data Injection (FDI) attacks. A mathematical formulation is developed for deriving the safe operating region of a PV system, and then, the mathematical formulation is further extended to determine a stability index at the Point of Common Coupling (PCC) of the PV system. In particular, the observation of a negative stability index at the PCC is evidence of an anomaly, and once an anomaly is detected, immediate corrective actions are adopted to prevent security breaches for grid-connected PV systems. The correlation between the variations in the active power and reactive power measurements to power grids voltage at the PCC are utilized to accurately identify compromised grid-connected PV systems. Different operating conditions are considered to evaluate and verify the performance of the proposed PIDMS using dynamic simulation.

References

[1] F. Mohammadi and M. Neagoe, "Emerging issues and challenges with the integration of solar power plants into power systems," in *Proc. Sol. Energy Convers. Communities*, 2020, pp. 157–173.

[2] C. Mehdipour and F. Mohammadi, "Design and analysis of a stand-alone photovoltaic system for footbridge lighting," *J. Sol. Energy Eng.*, vol. 4, no. 2, pp. 85–91, Jun. 2019.

[3] F. Mohammadi, G.-A. Nazri, and M. Saif, "A fast fault detection and identification approach in power distribution systems," in *Proc. IEEE Int. Conf. Power Gener. Syst. Renewable Energy Technol.*, 2019, pp. 1–4.

[4] F. Mohammadi et al., "Robust control strategies for microgrids: A review," *IEEE Syst. J.*, vol. 16, no. 2, pp. 2401–2412, Jun. 2022.

[5] T. T. Nguyen and F. Mohammadi,, "Cyber-physical power and energy systems with wireless sensor networks: A systematic review," *J. Elect. Eng. Technol.*, vol. 18, no. 6, pp. 4353–4365, Apr. 2023.

[6] T. O. Olowu, A. Sundararajan, M. Moghaddami, and A. I. Sarwat, "Future challenges and mitigation methods for high photovoltaic penetration: A survey," *Energies*, vol. 11, no. 7, Jul. 2018, Art. no. 1782.

[7] F. Mohammadi, "Emerging challenges in smart grid cybersecurity enhancement: A review," *Energies*, vol. 14, no. 5, Mar. 2021, Art. no. 1380.

[8] F. Mohammadi, M. Sanjari, and M. Saif, "A real-time blockchain-based multifunctional integrated smart metering system," in *Proc. IEEE Kansas Power Energy Conf.*, 2022, pp. 1–3.

[9] F. Mohammadi and R. Rashidzadeh, "Impact of stealthy false data injection attacks on power flow of power transmission lines–A mathematical verification," *Int. J. Elect. Power Energy Syst.*, vol. 142-A, Nov. 2022, Art. no. 108293.

[10] S. Hossain-McKenzie et al., "Proactive intrusion detection and mitigation system: Case study on packet replay attacks in distributed energy resource systems," in *Proc. IEEE Power Energy Conf. Illinois*, 2021, pp. 1–6.

[11] J. Johnson, "Roadmap for photovoltaic cyber security," Sandia Nat. Lab., Albuquerque, NM, USA, Sandia Tech. Rep., SAND 2017- 13262, Dec. 2017.

[12] 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-Phys. Syst.: Theory Appl.*, vol. 5, no.3, pp. 274–282, Mar. 2020.

[13] A. Houari, H. Renaudineau, J.-P. Martin, S. Pierfederici, and F. Meibody-Tabar, "Flatness-based control of three-phase inverter with output LC filter," *IEEE Trans. Ind. Electron.*, vol. 59, no. 7, pp. 2890–2897, Jul. 2012.

[14] H. Komurcugil, N. Altin, S. Ozdemir, and I. Sefa, "Lyapunov-function and proportional-resonant-based control strategy for single-phase grid-connected VSI with LCL filter," *IEEE Trans. Ind. Electron.*, vol. 63, no. 5, pp. 2838–2849, May 2016.

[15] S. Sahoo, T. Dragevi, Y. Yang, and F. Blaabjerg, "Adaptive resilient operation of cooperative grid-forming converters under cyber attacks," in *Proc. IEEE CyberPELS*, 2020, pp. 1–5.

[16] J. Zhang, J. Ye, and L. Guo, "Model-based cyber-attack detection for voltage source converters in Island microgrids," in *Proc. IEEE Energy Convers. Congr. Expo.*, 2021, pp. 1413–1418.

[17] C. B. Jones, A. R. Chavez, R. Darbali-Zamora, and S. Hossain-McKenzie, "Implementation of intrusion detection methods for distributed photovoltaic inverters at the grid-edge," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf.*, 2020, pp. 1–5.

[18] M. M. Rathore, A. Ahmad, and A. Paul, "Real time intrusion detection system for ultra-high-speed Big Data environments," *J. Supercomputing*, vol. 72, pp. 3489–3510, Feb. 2015.

[19] M. Mahdavisharif, S. Jamali, and R. Fotohi, "Big data-aware intrusion detection system in communication networks: A deep learning approach," *J. Grid Comput.*, vol. 19, pp. 1–28, Oct. 2021.

[20] A. Yayla, L. Haghnegahdar, and E. Dincelli, "Explainable artificial intelligence for smart grid intrusion detection systems," *IT Professional*, vol, 24,, no. 5, pp. 18–24, Sep./Oct. 2022.

[21] Q. Li, F. Li, J. Zhang, J. Ye, W. Song, and A. Mantooth, "Data-driven cyberattack detection for photovoltaic (PV) systems through analyzing micro-PMU data," in *Proc. IEEE Energy Convers. Congr. Expo.*, 2020, pp. 431–436.

[22] F. Li et al., "Detection and identification of cyber and physical attacks on distribution power grids with PVs: An online high-dimensional data-driven approach," *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 1, pp. 1282–1291, Feb. 2022.

[23] J. Zhang, Q. Li, J. Ye, and L. Guo, "Cyber-physical security framework for photovoltaic farms," in *Proc. IEEE CyberPELS*, 2020, pp. 1–7.

[24] Y. Dubasi, A. Khan, Q. Li, and A. Mantooth, "Security vulnerability and mitigation in photovoltaic systems," in *Proc. IEEE 12th Int. Symp. Power Electron. Distrib. Gener. Syst.*, 2021, pp. 1–7.

[25] J. Ramos-Ruiz et al., "An active detection scheme for cyber attacks on grid-tied PV systems," in *Proc. IEEE CyberPELS*, 2020, pp. 1–6.

[26] K. Jhala, P. Pradhan, and B. Natarajan, "Perturbation-based diagnosis of false data injection attack using distributed energy resources," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1589–1601, Mar. 2021.

[27] B. Kang et al., "Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations," in *Proc. IEEE Conf. Emerg. Technol. Factory Automat.*, 2015, pp. 1–8.

[28] A. Peedikayil Kuruvila, I. Zografopoulos, K. Basu, and C. Konstantinou, "Hardware-assisted detection of firmware attacks in inverter-based cyber-physical microgrids," *Int. J. Elect. Power Energy Syst.*, vol. 132, Nov. 2021, Art. no. 107150.

[29] G. Bere, B. Ahn, J. J. Ochoa, T. Kim, A. A. Hadi, and J. Choi, "Blockchain-based firmware security check and recovery for smart inverters," in *Proc. IEEE Appl. Power Electron. Conf. Expo.*, 2021, pp. 675–679.

[30] P. M. Rezayi, M. R. Zolghadri, F. Mohammadi, and A. Rezaei-Zare, "PLL-Less active and reactive power controller for three-phase grid-connected power converters," in *Proc. IEEE Int. Conf. Environ. Elect. Eng.,* 2022, pp. 1–6.

[31] F. Mohammadi, R. Bok, M. Hajian, and A. Rezaei-Zare, "Controller-hardware-in-the-Loop testing of a single-phase single-stage transformerless grid-connected photovoltaic inverter," in *Proc. IEEE Texas Power Energy Conf.*, 2022, pp. 1–6.

[32] S. Sourav, P. P. Biswas, B. Chen, and D. Mashima, "Detecting hidden attackers in photovoltaic systems using machine learning," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids*, 2022, pp. 360–366.

[33] S. Jadidi, H. Badihi, and Y. Zhang, "Active cyber-resilient control for a PV system at microgrid level," in *Proc. IEEE 4th Int. Conf. Renewable Energy Power Eng.*, 2021, pp. 339–344.

[34] Z. Shen, W. Xu, W. Li, Y. Shi, and F. Gao, "Digital twin application for attack detection and mitigation of PV-Based smart systems using fast and accurate hybrid machine learning algorithm," *Sol. Energy*, vol. 250, pp. 377–387, Jan. 2023.

[35] A. Basati, J. M. Guerrero, J. C. Vasquez, N. Bazmohammadi, and S. Golestan, "A data-driven framework for FDI attack detection and mitigation in DC microgrids," *Energies*, vol. 15, no. 22, Nov. 2022, Art. no. 8539.