smart cities

MDPI

Article

Smart Grid Resilience for Grid-Connected PV and Protection Systems under Cyber Threats

Feras Alasali [1,*], Awni Itradat [2], Salah Abu Ghalyon [2], Mohammad Abudayyeh [1], Naser El-Naily [3], Ali M. Hayajneh [1] and Anas AlMajali [2]

[1] Department of Electrical Engineering, Faculty of Engineering, The Hashemite University, Zarqa 13133, Jordan; mohammedabudayyeeh2001@gmail.com (M.A.); alihayajneh@hu.edu.jo (A.M.H.)
[2] Department of Computer Engineering, Faculty of Engineering, The Hashemite University, P.O. Box 330127, Zarqa 13133, Jordan; itradat@hu.edu.jo (A.I.); salah.g.ghalyon@hu.edu.jo (S.A.G.); almajali@hu.edu.jo (A.A.)
[3] Department of Electrical Technology, College of Electrical and Electronics Technology-Benghazi, Benghazi 5213, Libya; naseralnaile222@gmail.com
* Correspondence: ferasasali@hu.edu.jo

Abstract: In recent years, the integration of Distributed Energy Resources (DERs) and communication networks has presented significant challenges to power system control and protection, primarily as a result of the emergence of smart grids and cyber threats. As the use of grid-connected solar Photovoltaic (PV) systems continues to increase with the use of intelligent PV inverters, the susceptibility of these systems to cyber attacks and their potential impact on grid stability emerges as a critical concern based on the inverter control models. This study explores the cyber-threat consequences of selectively targeting the components of PV systems, with a special focus on the inverter and Overcurrent Protection Relay (OCR). This research also evaluates the interconnectedness between these two components under different cyber-attack scenarios. A three-phase radial Electromagnetic Transients Program (EMTP) is employed for grid modeling and transient analysis under different cyber attacks. The findings of our analysis highlight the complex relationship between vulnerabilities in inverters and relays, emphasizing the consequential consequences of affecting one of the components on the other. In addition, this work aims to evaluate the impact of cyber attacks on the overall performance and stability of grid-connected PV systems. For example, in the attack on the PV inverters, the OCR failed to identify and eliminate the fault during a pulse signal attack with a short duration of 0.1 s. This resulted in considerable harmonic distortion and substantial power losses as a result of the protection system's failure to recognize and respond to the irregular attack signal. Our study provides significant contributions to the understanding of cybersecurity in grid-connected solar PV systems. It highlights the importance of implementing improved protective measures and resilience techniques in response to the changing energy environment towards smart grids.

Keywords: smart grid; cyber threats; PV; overcurrent relay; intelligent inverter

Citation: Alasali, F.; Itradat, A.; Abu Ghalyon, S.; Abudayyeh, M.; El-Naily, N.; Hayajneh, A.M.; AlMajali, A. Smart Grid Resilience for Grid-Connected PV and Protection Systems under Cyber Threats. *Smart Cities* **2024**, *7*, 51–77. https://doi.org/10.3390/smartcities7010003

Academic Editor: Antonio Moreno-Munoz

Received: 12 November 2023
Revised: 3 December 2023
Accepted: 4 December 2023
Published: 22 December 2023

1. Introduction

1.1. Motivation

The integration of DERs based on renewable energy sources into power systems is steadily increasing due to significant advancements in technology because of their clean and cost-effective energy production [1]. As a result, electrical power grid utilities continue to install various types of intelligent electronic devices (IEDs), such as power meters, inverters, and protective relays. The expansion of the market shares of DERs has increased the measurements that rely on communications between IEDs both inside and outside the substation boundary. To ensure safe operation in modern and smart power grid systems, it is necessary to maintain complex interactions between smart devices and physical grid components [1,2].

In smart grids, the rise of information and communication-based control approaches has raised cybersecurity-related concerns. Smart PV inverters include advanced power electronic devices such as microcontrollers, digital signal processors, and Integrated Circuits (ICs), which are vulnerable to a wide range of cyber attacks including data integrity attacks and communication-based attacks. Furthermore, a lack of firmware upgrades of PV plants has led to the abnormal behaviors of these inverters, such as random power factor adjustments, voltage fluctuations, etc. [3]. In modern control approaches, these inverters can be remotely managed via a SCADA system that communicates primarily through Ethernet, fiber, or other wireless communications [4,5]. These communication mechanisms are susceptible to cyber attacks, which have the potential to give unauthorized individuals power over the entire system, preventing operators from having control over the system converters [6]. In addition, protection relays, such as IEDs, are responsible for detecting and clearing contingent events occurring in the system using various protection methods. These events in electrical power systems can cause system damage or at least impact the life cycle of the components and appliances [5,6]. The relay commands are sent using the GOOSE protocol, which offers a faster response of the backup protection.

Generally, there is a lack of research on the resilience of smart PV inverters and protection systems under cyber-physical threats using real power distribution network specifications. In addition, according to the literature review, the transient phenomena in electrical systems under cyber attacks for smart PV inverters and protection systems have not been considered and investigated. Therefore, this research focuses on investigating different cyber-physical threat concerns for smart PV control inverters and OCR protection schemes by using the Electromagnetic Transients Program (EMTP).

1.2. Literature Review

In smart grid and modern power network models, efficient power delivery to the wheel relies significantly on the importance and need of smart energy management for the DER, such as PV, fuel cell–battery, and electric vehicle [7]. Online improvement of energy management for the grid control settings is important [8]. Therefore, the power systems industry is now experiencing a significant transformation due to the incorporation of advanced technologies, namely in the areas of smart PV inverters, protection, and cyber-physical security. In recent years, there has been a notable increase in research efforts aimed at understanding the vulnerabilities, hazards, and possible measures to mitigate risks related to modern and smart electricity systems. This section offers a detailed examination of several studies conducted to explore the effects of cyber-physical threats on smart grids with grid-connected PV systems. The authors of [9] provided a comprehensive description of the principal controller, known as consensus-based control, which is responsible for controlling active and reactive power in a microgrid. The findings showed that when there is a variance in reference values at the nodes, the distributed architecture is capable of achieving realistic power allocation based on the rated power ratio. The control process only takes place among the nodes that possess unconstrained accessible resources, resulting in convergence towards an uncontrolled average voltage level.

In [10], a distributed control system was developed specifically for managing active power and frequency dynamics within a microgrid. The researchers investigated the stability of the divided system by examining the connections that are essential for communication and physical operations. However, the delays in the cyber layer were not taken into consideration. The authors of [11] provided a distributed control system that does not use droop control but instead utilizes a robust distributed controller. The proposed controller is specifically designed to facilitate the sharing of active and reactive power across subsystems that consist of several DERs. However, the potential effects of communication, the cyber layer, and control convergence remain unaddressed by [9–11]. The literature reviews found in [10–12] discussed various PV controllers in microgrids. These controllers were characterized by their reliance on communication-based and control strategies. Additionally, the microgrids operated in conjunction with droop control and

occasionally employed droop-free systems. The authors of [12] examined various scenarios of communication architecture, typically focusing on single, predetermined delays limited to tiny communication networks.

A limited number of researchers have explored the consequences of cyber attacks on smart power networks with DERs, particularly Photovoltaic (PV) systems. The investigation by Sowa and Monti [13] examined a consensus-based control strategy for islanded microgrids that takes into account the dynamics of both the cyber and physical layers. The proposed control scheme was developed to handle any electrical and communication topologies with varying characteristics. The control method successfully achieved the main and secondary control objectives for islanded microgrids inside a unified control layer. The suggested cyber model was designed and analyzed to incorporate the physical and cyber levels, as well as the dynamics of both layers and their interconnections. The goal of robustness was achieved by including and mitigating uncertainties within the model. However, the potential effects caused by communication, the cyber layer, and control convergence under different cyber-attack scenarios were not adequately acknowledged or investigated. Majumder et al. [14] determined in their work the sub-categorization of each communication and the physical and cyber domain component, specifically focusing only on describing the various cyber attacks on the communication and physical layers. In another study, Liu and Li [15] investigated the cyber-physical threats of a microgrid equipped with grid-forming inverters and considered low short-circuit levels. The authors of [15] did not consider and investigate different attack scenarios, real network parameters, and protection devices.

Furthermore, the integration of inverters into distribution networks will result in chaining the fault behavior and an increase in fault current, leading to the potential misoperation of protection relays, specifically the OCR [6]. The OCR aims to maintain continuous monitoring of the electrical current at the grid. In the event that the current exceeds the predetermined threshold, known as the pickup setting, the relay sends a trip signal to the circuit breaker. The primary emphasis of this work is to investigate the impact of cyber-physical threats on smart inverters, which might effectively decrease or increase fault currents to levels below the pickup setting, hence mitigating blinding misoperations [4,6]. In addition, this study also examines the impact of PV irradiance within normal operation on the voltage and current of a PV system, which exhibit variations throughout the day. Table 1 presents a detailed summary of recent studies that enhance smart grid resilience for cyber threats with DER systems [16–24]. In general, the studies [19–21] focused on studying the impact of cyber attacks on power protection systems, while [5,15] investigated the impact of cyber threats on microgrid control systems. In another study, Zaki et al. [25] discussed the growing difficulties in protecting active distribution networks due to the increased integration of PV-generating units. They suggested a fault identification strategy in [25] to consider the unique characteristics of PV systems and uncertainties. Oliveira-De Jesus and Sorrentino [26] proposed a new approach to evaluate the distributed faults and coordination of OCR solutions in transmission lines, utilizing time dial and pickup settings. However, a limited number of studies have examined both protection and PV control models. Therefore, this work takes into consideration the research gaps that have been discovered in the current literature, as shown in Table 1. Firstly, different cyber-attack scenarios are employed to investigate their impact on power protection and smart PV controllers. Secondly, this work aims to examine different cyber attacks on a real network model. Finally, our goal is to analyze transient phenomena for a real power system, including transients and non-steady-state events that can occur for many reasons, including switching operations, faults, or other disturbances. In this work, the Electromagnetic Transients Program (EMTP), is used. The EMTP helps in understanding how electrical systems behave during transient events. As this work aims to assess the stability of power systems, the EMTP was chosen because of its ability to simulate and analyze factors such as voltage stability, rotor angle stability, and small-signal stability, which act as important indicators of the reliable operation of power networks.

Table 1. Detailed summary of recent studies that enhance smart grid resilience for cyber threats with DER systems.

Ref.	Year	Protocol	Type of Cyber Attack	Study Area		Standard or Real Network	(DERs) TYPE	Physical Software	Cyber Software
				Protection System	Control System				
[3]	2019	PMU	Data spoofing, Man-in-the-Middle (MITM)	√	×	IEEE-14	×	Real-Time Digital Simulator (RTDS)	√
[4]	2020	×	False Data Injection (FDI)	×	√	IEEE-8500	PV	OpenDSS and MATLAB	×
[5]	2023	×	Stealthy Data Integrity Attacks (DIA)	×	√	IEEE-34	PV	Real-time Typhoon testbed	×
[6]	2023	×	FDI attacks and Denial of Service (DOS)	√	×	IEEE-14	×	MATLAB/Simulink	×
[7]	2023	IEC61850	FDI	√	×	CIGRE	PV	Real-Time Digital Simulator (RTDS)	×
[16]	2023	×	DoS, intermittent attack, and modification attacks	×	√	×	PV	Power Hardware-2in-the-Loop (P-HIL) test	×
[17]	2023	PMUs	DoS and DIA	×	√	IEEE-14	PV	EMTP MATLAB/Simulink	×
[18]	2023	PMUs	DIA, replay attacks, Sophisticated attacks	×	√	IEEE-37	PV	OPAL-RT	×
[19]	2023	IEC61850	FDI and DOS	√	×	×	×	OPAL-RT	×
[20]	2023	IEC 61850	FDI, DOS	√	√	IEEE-34 bus	PV	OPAL-RT	√
[21]	2023	×	FDI	√	×	IEEE-118 bus,	×	MATLAB	×
[22]	2023	×	DIA	×	√	Microgrid benchmark	PV	×	×
[15]	2023	PMUs	DOS	×	√	28 bus test system	PV	MATLAB	×
[23]	2023	IEC61850	FDIA	√	√	×	PV	OPAL-RT.	×
[24]	2023	GOOSE	FDIA	√	×	×	×	MATLAB/Simulink	×
Proposed study		IEC61850 GOOSE	FDI, DOS, MITM	√	√	Realistic power grid	PV	EMTP	√

1.3. Contributions

The key findings and contributions of this study can be summarized as follows:

- Examine and investigate the impact of different cyber attacks (FDI, DOS, and MITM) on smart PV control and modern OCR protection systems within the IEC61850 and GOOSE protocols.
- Provide insights into the electrical and electromagnetic aspects of the cyber attack's impact on a real network parameter.
- Assess the consequences of the cyber attack on the power grid on the transient behavior of the smart PV control and modern OCR protection systems.
- Model a realistic power network using EMTP for studying transient events and periods under different grid operation scenarios: normal operation, normal operation with

irradiation drops, various cyber attacks at smart inverters, and OCR during physical fault conditions.

The remainder of this work is organized as follows: Section 2 presents the problem statement and methodology. Section 3 introduces the proposed smart power network and cyber modeling. Section 4 introduces the results of the adaptive OCRs and smart-grid-connected inverters under different fault and cyber-attack scenarios. Finally, the summary of this study is presented in Section 5.

2. Problem Statement and Power Grid Methodology

This research focuses on the development and evaluation of a modern adaptive protection OCR system. Adaptive OCR schemes adjust their settings based on the network topology between traditional power networks and grid-connected PV modes. Initially, breaker statuses and grid information determine the network's mode (grid-connected or islanding). A continuous monitoring process compares the current network topology to its previous state, utilizing stored settings if unchanged. The selected OCR group settings for primary relay (OCRP) and Backup relays (OCRB), emphasizing heightened sensitivity and selectivity, are implemented through communication links, as shown in Figure 1. The OCR setting is selected to achieve the total tripping time for OCRs during the fault event. The OCR tripping is obtained by solving Equation (1):

$$T = \left[\frac{A}{\left(\frac{I_{fault}}{I_{Pick}}\right)^{B} - 1} TMS \right] \quad (1)$$

where T is the OCR tripping time, A and B are the constant of the relay characteristic, I_{fault} is the fault current, I_{Pick} is the pickup current, and the TMS is Time Multiplier Setting. Figure 1 illustrates a radial system scenario using adaptive OCRs. If a fault occurs in one of the lines, the primary relay (OCRP) is responsible for detecting the fault and disconnecting the faulty line by tripping it. If the OCRP fails to trip the fault and isolate a healthy line in a particular fault scenario, the backup relay (OCRB) will activate with enough coordination time. For example, the time tripping at current fault (I_{fault}) equal to 2000 A for the OCRP adjusts its setting of I_{Pick} equal to 50 A to cover the load and cable thermal constraints, and the IEC normal standard characteristic curve (A equal to 0.14 and B equal to 0.02) and TMS equal to 0.01 will be $T = \left[\frac{0.14}{\left(\frac{2000}{50}\right)^{0.02} - 1} 0.01 \right] = 0.018$ s. The backup OCRB will operate at time equal to 0.318 as the coordination time interval is equal to 0.3 s. Nevertheless, a cyber attack that changes the adaptive relay configuration, blocks the relay trip signal, or results in communication failure might result in a disconnect of functional lines from the network, power problems, damage, and disconnection of the DER. Consequently, the network's stability and energy supply will be negatively impacted.

In addition, the power system configuration of a grid-connected inverter with existing physical faults and cyber threats is shown in Figure 1. The modeling of smart-grid-following inverter controls involves a number of components such as the Phase-Locked Loop (PLL), filter, power controller, and current controller. These components are often built inside the d_q reference frame (direct-quadrature or synchronous). The PLL aims to measure the real frequency of the system (f) and synchronizes the estimated frequency to produce the transformation angle. In this study, the dynamics of the smart-grid-following inverter model is illustrated in Figure 1, which is represented in a local d_q-synchronous reference frame, including the transformation angles that determine the separate synchronous reference frames (θ). Then, the active and reactive power (P_{grid}, Q_{grid}) are calculated and fed to the outer-loop controller. The outer-loop controller aims to generate a reference control signal to the inner-loop control by comparing the P_{grid}, Q_{grid} and voltage U_C and a reference signal. This controller, as the power controller, aims to regulate the output power by selecting the output current references for the inner-loop controller. The system

dynamics as a whole are contingent upon the dynamics of the inverter in conjunction with the current limiting method in the inner-loop controller. Finally, the control signal from the inner-loop controller will be fed to Sinusoidal Pulse-Width Modulation (SPWM) to control the smart inverter, as described in detail in [27].

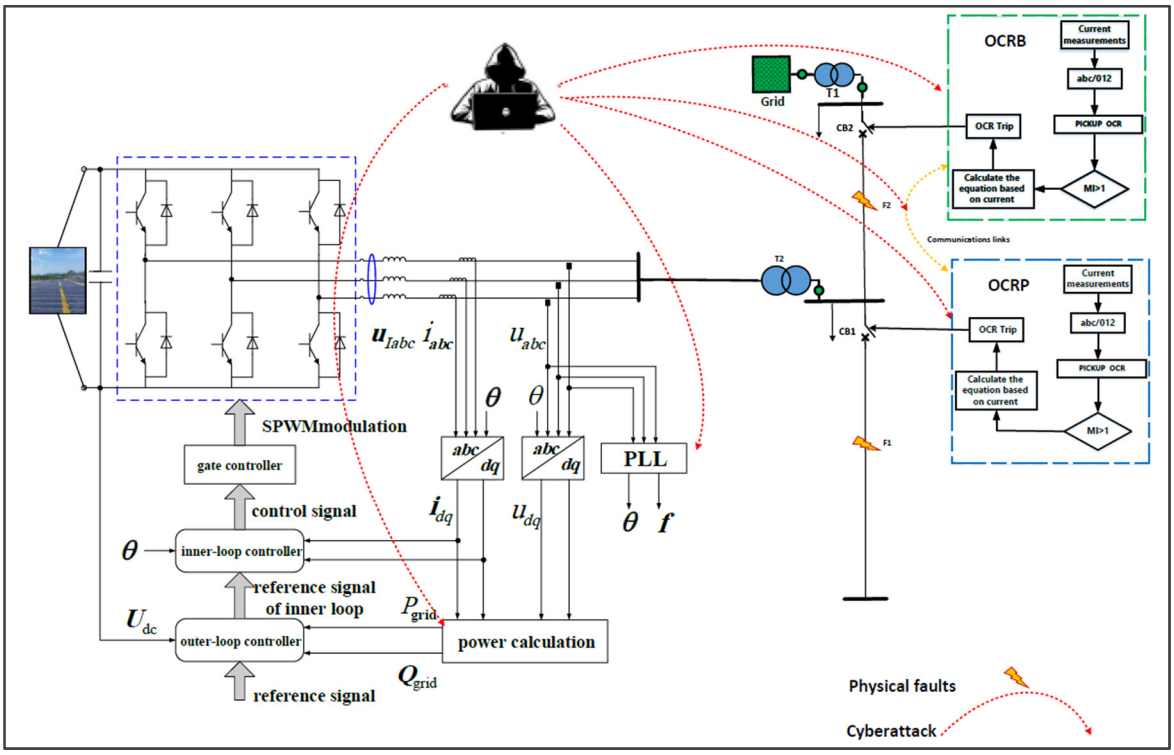

Figure 1. The power system configuration of grid-connected inverter and OCRs with existing physical faults and cyber threats.

Within the framework of the grid-connected inverter, the OCRs show effectiveness in identifying faults by elevated levels of overcurrent. The thorough analysis demonstrated here enhances understanding of the many cyber threats and fault scenarios that might occur in the grid-connected inverter-based smart grid. The use of a communication architecture between the central control and local controls (inverters) is an increasingly common technique within the field of smart grid control systems. The implementation of protocols such as IEC61850, and Modbus is a key aspect of this process [15,27]. Nevertheless, having a number of vulnerabilities in the cyber layer presents substantial hazards. The possibility for attackers to exploit an unsecured communication network, which is defined by a lack of communication protocols with integrated cyber capabilities, insufficient firewalls, and insufficient security measures, is a significant concern.

3. Proposed Smart Power Network and Cyber Modeling

In real power systems and smart grids, the transient phenomena issues are non-steady-state events that can happen for a number of reasons, such as switching processes or faults. In this work, the Electromagnetic Transients Program (EMTP) is used to examine the power network performance under cyber attack. The EMTP enables it to be simple to fully understand how electrical systems react to short-term events, as shown in Figure 1. The EMTP is a commonly used method for obtaining transient solutions in the fields of power systems and power electronics [28]. This simulation includes all possible electrical conditions and express network equations using differential equations. In the EMPT, the reactance characteristics of capacitive and inductive elements demonstrate changes that rely on the frequency. This requires the development of comprehensive models for electrical components and controllers [28,29]. By utilizing time intervals of less than 50 microseconds,

the EMTP model succeeds at illustrating the sudden dynamics occurring within the power system caused by power electronic equipment such as voltage source converters. In the model power network and smart grids with a DER, the converters are commonly utilized as connectors between the DER and distribution grids. The EMTP simulation plays an increasingly important role in investigating the integration of renewables into modern power networks. This consists of activities such as control system design, investigation of stability, and coordination of protective mechanisms. In addition, the time scale of operation of power protection relays and PV inverters is considered in the area of electromagnetic transient phenomena, as shown in Figure 2. Therefore, it is important to investigate the impact of different cyber threats in the real power system and smart grids within transient phenomena statutes.

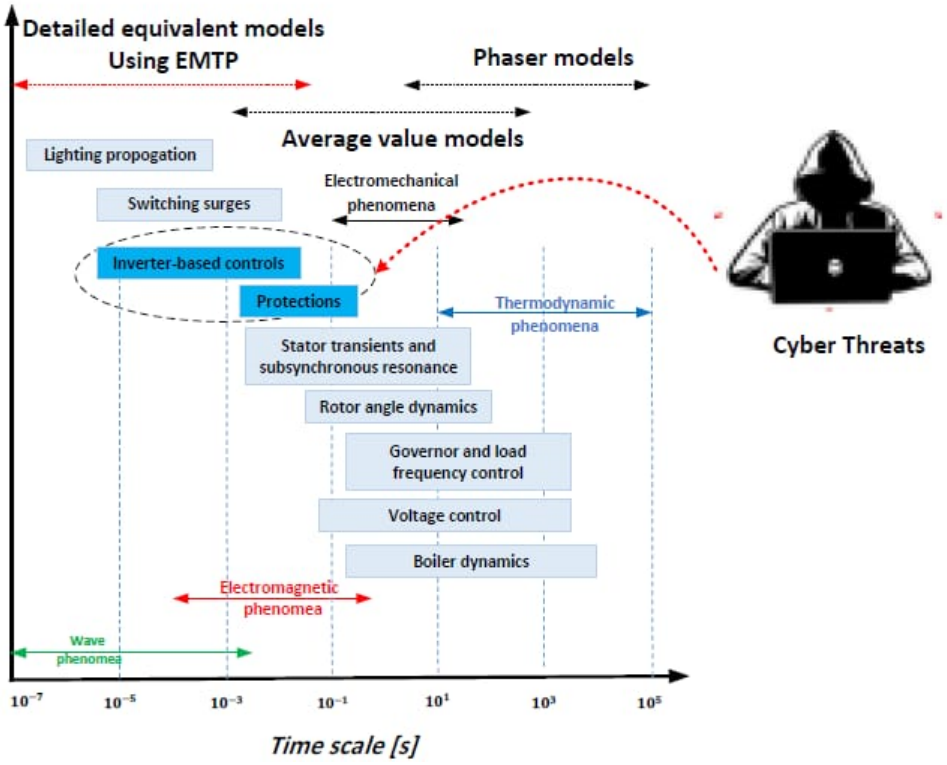

Figure 2. The EMTP models for different applications.

3.1. The Proposed Smart Power Grid Model

The power grid used in this study mimics a real power grid. This grid is simulated using the EMTP tool, as illustrated in Figure 3. The network includes a mix of conventional electricity sources, signified by a local power company line (Bus 10 (33 KV)), and a PV farm with a total capacity of 4 MWp and links to the 33 KV bus via four power transformers (T15 to T18). This farm comprises four distinct zones denoted as P1 to P4 with a capacity of 1 MWp for each one, as illustrated in Figure 3. In addition, the grid-connected PV system (G1 to G9) to the low-voltage side of the power network significantly contributes to meeting the energy needs of the network, as described in Table 2. As shown in Figure 3, the power network is protected using 12 OCRS. Two primary 33/11 KV transformers (T13 and T14), as depicted in Figure 3, provide power to the LV network. Subsequently, 12 distribution transformers (T1 to T12: 11/0.415 KV) distribute the necessary power to the 37 buildings, denoted as B1 to B37. The expansive LV power network encompasses an area of roughly 34,475 km^2, including 37 buildings and supporting an annual energy consumption of nearly 8.5 GWh, as described in Table 3.

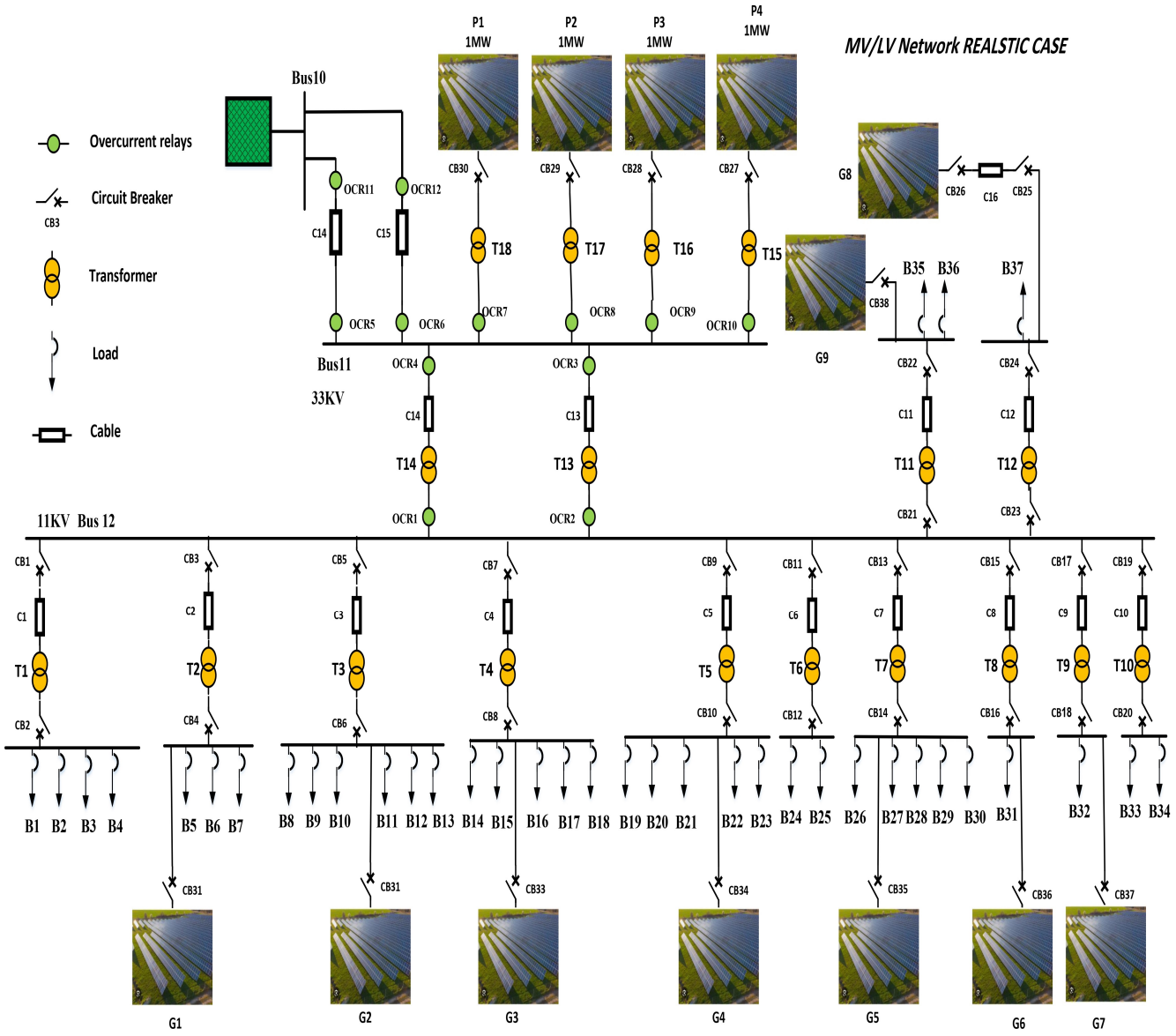

Figure 3. The proposed smart power network.

Table 2. Details of the PV systems in the proposed power grid.

Area	PV Power (KWp)	Energy Production (kWh/Year)
P1	1011.84	1,880,504
P2	1011.84	1,880,504
P3	1011.84	1,880,504
P4	980.22	1,821,738
G1	22.320	36.873
G2	22.320	36.873
G3	22.320	36.873
G4	22.320	36.873
G5	23.560	41.324
G6	13.640	23.925
G7	22.940	38.310
G8	23.560	39.345
G9	22.320	41.939

Table 3. Detailed load demand based on CB ratings in the proposed power grid.

Building	CB Rating	Building	CB Rating
B1	1250	B19	400
B2	600	B20	400
B3	125	B21	125
B4	125	B22	250
B5	1250	B23	250
B6	400	B24	2500
B7	60	B25	2500
B8	150	B26	400
B9	200	B27	1250
B10	125	B28	250
B11	400	B29	400
B12	200	B30	250
B13	400	B31	800
B14	250	B32	3200
B15	400	B33	2000
B16	250	B34	2500
B17	160	B35	2500
B18	400	B36	2500
		B37	3200

3.2. Cyber-Attack Modeling

The IEDs in smart grids exchange messages using the GOOSE protocol to provide high-speed communication for exchanging critical information. Critical events in power system protection and inverter control applications, such as inter-trip and blocking, need to be delivered in less than 3 ms of time [18]. Therefore, GOOSE messages are directly attached to the data link layer using the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) protocol. Furthermore, by leveraging Ethernet switch technology, the GOOSE protocol can implement CSMA/CD in multicast and full-duplex modes for transmitting and receiving messages, making it suitable for real-time and mission-critical tasks, including protection and grid-connected PV applications. IEDs can broadcast messages to multiple receivers at the same time when they detect new events [19,20]. The GOOSE protocol is equipped with two distinct retransmission mechanisms to ensure message reliability: steady-state retransmission and fast-retransmission mechanisms. These mechanisms rely on the Status (ST) number and the Sequence (SQ) number, where an increase in ST signifies a new event, while an increase in SQ indicates a repetition of the same GOOSE message [21,22]. In this study, we examine several cyber attacks on control systems (smart PV inverters) and on protection systems (OCR), their cascading effects on each other, and, ultimately, the overall grid stability, as presented in Table 4. The proposed attacks fall in three categories:

- Man-in-the-Middle (MITM): The attacker gains access to communication channels, enabling them to delay or block certain messages.
- False Data Injection (FDI): This attack violates the system's integrity by injecting fabricated data to alter the setpoints and protection setting.
- Denial-of-Service (DOS) Attack: The attacker isolates one or several grid components, preventing them from acting according to the fault occurrence, which will compromise the stability of the grid.

Table 4. Summary of the vulnerability and cyber attacks at the proposed smart grid.

Vulnerability	Description	Relevance to Cyber Attacks
Vulnerabilities in Communication Architecture	Using protocols like IEC61850 that has loose cyber constraints and insufficient security measures.	FDI: Exploitation of un-encrypted communication DOS: Exposed to denial of service.
Vulnerabilities in Smart Inverter Control Method	Susceptibility to manipulation by cyber attacks.	FDI: Manipulation of values and set points, creating misleading reference values for control.
Vulnerabilities in Adaptive OCR Systems	Issues related to communication failure or cyber risks, such as prevention or delay of the OCR action will affect the grid stability.	MITM: Delaying fault messaging prevention or delay of changing group settings by adaptive OCRs. DOS: Dropping order messages preventing OCRs from acting on faults.

3.2.1. Cyber Threats on Power Protection System (OCR)

Intelligent OCRs play a vital role in the protection system of a power grid. They are responsible for detecting fault occurrences in the grid and ensuring rapid isolation of the affected segments of the power grid. In order to facilitate effective coordination, these relays commonly include a backup relay (OCRB) positioned upstream of the primary protective system (OCRP), as shown in Figure 3. However, in Distributed Network (DN) systems with many DER locations, the implementation of protective mechanisms becomes more complex [2,3]. Therefore, adaptive OCR systems are necessary to accommodate the dynamic fluctuations in topology, generation, and load by changing and using different relay setting groups [6]. This is because traditional protection strategies may be insufficient in addressing these changes [6,7]. The implementation of adaptive protection schemes presents a substantial difficulty, namely in relation to communication failure, storage of protective settings, operational curve functions, and cyber risks. Therefore, any prevention or delay of the action of the relay can affect the grid stability. In this work, three main cyber-attack vectors are employed to target the protection system in Figure 2:

- Manipulating Group Settings: The attacker does not allow the adaptive OCRs to change the group setting or postpone that change for a certain amount of time (FDI).
- Delaying Fault Messaging: The attacker's goal is to delay the communication carrying information about a detected physical fault by using the MITM attack. Such a scenario can lead to instability of the grid as it loses the ability to respond in time for any fault.

3.2.2. Cyber Threats on the Smart PV Inverters

The comprehensive analysis presented in this study enhances the understanding of potential cyber threats and fault scenarios in smart grids relying on grid-connected inverters. The incorporation of communication architecture between central control and local controls, particularly inverters, is a common practice in smart grid control systems, often employing protocols such as IEC61850 and Modbus, as shown in Figure 1 and Table 4 [15,27]. The existence of vulnerabilities in the cyber layer presents substantial risks, as an unsecured communication network lacking integrated cyber capabilities, inadequate firewalls, and insufficient security measures can be exploited by potential attackers, presenting a notable concern. This occurrence is susceptible to being manipulated by different cyber-attack approaches such as FDIAs. In the event of an attack on smart PV inverters and a change in the value of reactive power under normal conditions, according to IEEE-1547-2018 standards [5,15], the reactive power should not change under normal conditions. However, an attack occurring on the inverters, changing the reference value for reactive power, leads to a high current draw from the grid. This will lead OCR devices to detect the issue and

disconnect the main grid. The previously mentioned manipulation has the capability of bypassing the protective mechanisms in operation. It achieves this by modifying the values, creating misleading reference value control for the inner- and outer-loop control, thereby tricking the principal smart inverter control method. In order to simulate possible cyber threats, four types of attack signals, as described by [15], are defined as:

- Continuous Pulse Signal: The attacker has the ability to periodically introduce malicious vectors, which turn the transmitted data into a periodic square wave signal.
- Scaling Signal: This form of attack has the potential to modify the signal through the utilization of a scaling attack factor.
- Sine Signal: The original data are modified using a sinusoidal signal with an amplitude factor.
- Ramp Signal: The control signal will take the shape of a ramp waveform signal.

4. Results

The smart grid system, including adaptive OCRs and the smart-grid-connected inverter, as outlined in Section 2, has been modeled for the MV/LV network model, as shown in Figure 2. This MV/LV network has been built using actual network parameters and measurands, and their performance has been assessed in the event of various cyber attacks. The objective of this section is to show and analyze the transient results obtained through the number of physical fault scenarios. Initially, an assessment is conducted on the performance of the proposed power network without cyber-attack events and under an irradiation drop scenario. Subsequently, the impact of different cyber attacks on the performance of the protection system (OCR) and smart inverter is demonstrated. Furthermore, the transient outcomes of the proposed power network in terms of voltage, current, active power, and reactive power are demonstrated. Overall, this section examines the results of the simulated cyber attacks on the overall grid performance over a simulation time of one second (transient event). Therefore, a baseline performance is firstly established to record the grid's operation under normal conditions, without any faults or attacks. The main parameters that have been monitored during this evaluation include:

- The voltage on the PV bus (or the bus of Point of Common Coupling (PCC)).
- The DC voltage on the PV system (as measured on the inverter).
- The AC current of the PV system (as measured on the inverter).
- The level of the irradiation.
- The direct and quadratic current (I_d and I_q) at the grid.
- The active and reactive power at the grid.

4.1. The Proposed Power Network under Normal Operation Condition

In order to assess the performance of the proposed power grid and ensure suitable cyber threats across various attack scenarios, the grid was examined under normal operating conditions (prior to any cyber attacks or physical fault).

In this investigation, the operational performance of the PV system is evaluated under normal operating conditions, with constant load or irradiation and the exclusion of any attacks or faults. The irradiation level is maintained at a constant 1000 W/m^2, and the simulation duration is set to 1 s to cover the transient events the scope of this work, as shown in Figure 4. The results during the time of less than 0.04 s present the performance during the transient period of connecting the PV to the power grid. During the steady state, the findings indicate a stable power system with the voltage at the Point of Common Coupling (PCC) bus registering at 33 kV. The current within the PV system is measured at 25 A, facilitating an active power output of 1 MW. It is essential to note that the analysis focuses on a single PV unit. Additionally, the direct current component (I_d) remains constant at 1.25 A, while both reactive power and quadrature current (I_q) values are maintained at zero. This comprehensive examination underlines the robustness and

stability of the PV system under optimal operating conditions, providing essential insights into its performance metrics.

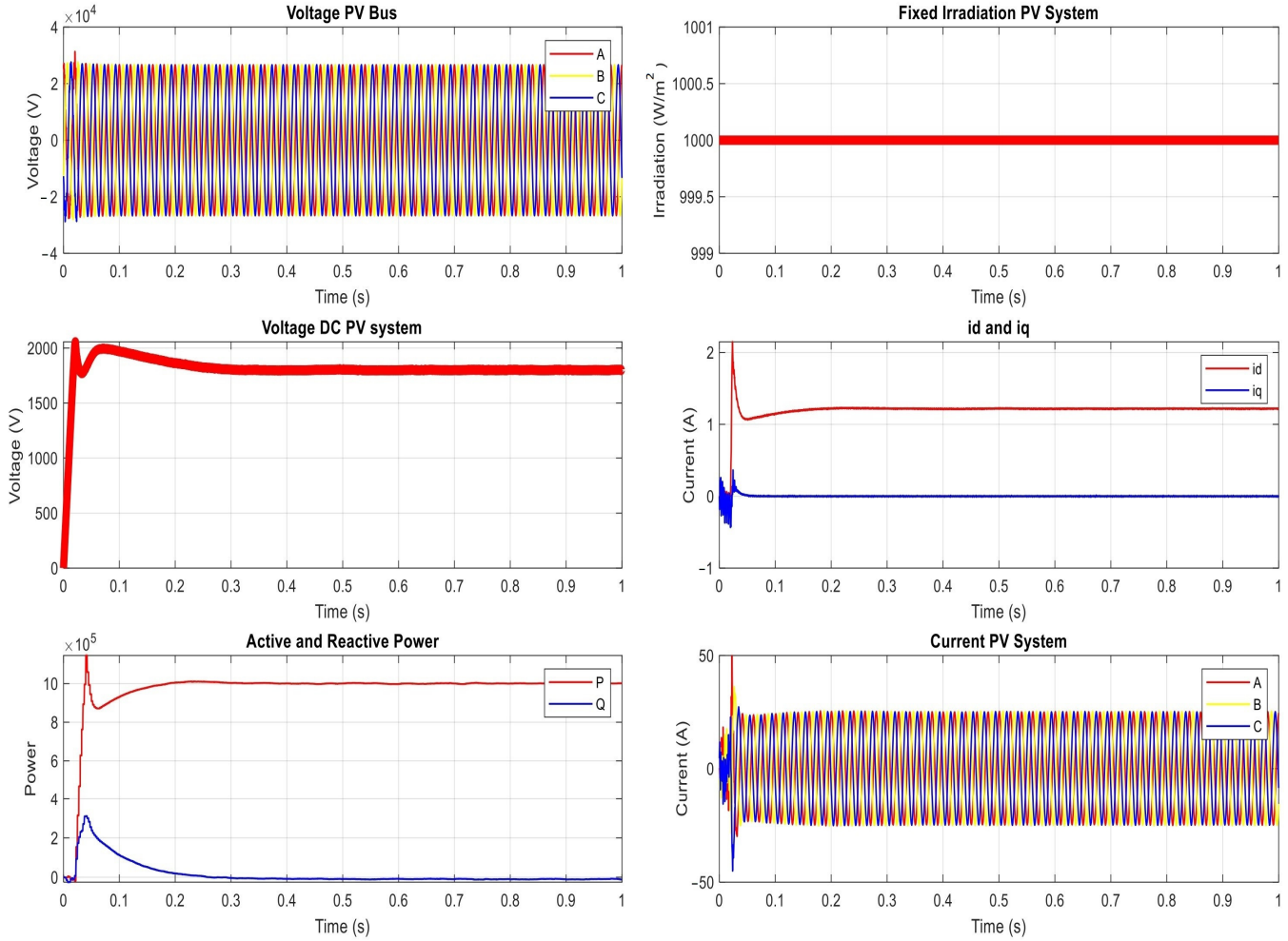

Figure 4. The results of the proposed power network under normal operation conditions with constant irradiation.

To evaluate the modeling of the proposed power network, the study examines the consequences of a reduction in irradiation levels on the operation of the PV system during normal operation scenarios. Therefore, at time 0.4 s, the irradiation level experienced a temporary decrease from the standard 1000 to 800 W/m^2 for a duration of 0.1 s, and then the irradiation increased to 900 W/m^2 for a duration of 0.2 s, as shown in Figure 5. The level of irradiation returned to its baseline value of 1000 W/m^2 throughout the remaining duration of the simulation. This resulted in a notable decrease in the DC voltage to 1500 V during the interval from time 0.4 to 0.5 s (with 800 W/m^2). The current within the PV system is measured at 17 A, facilitating an active power output of 0.7 MW. While the reactive power maintained a constant value of zero, fluctuations were evident in the active power. Subsequently, as the irradiation level increased to 900, the power ascended to 0.9 MW before returning to its initial level of 1 MW when the irradiation resumed its standard value of 1000. The observed power variations had a noticeable effect on the present values, which were impacted by the consistent voltage at the PCC. This comprehensive analysis offers significant insights into the dynamic behavior of Photovoltaic (PV) systems according to changes in irradiation levels, and how these changes affect power and current dynamics.

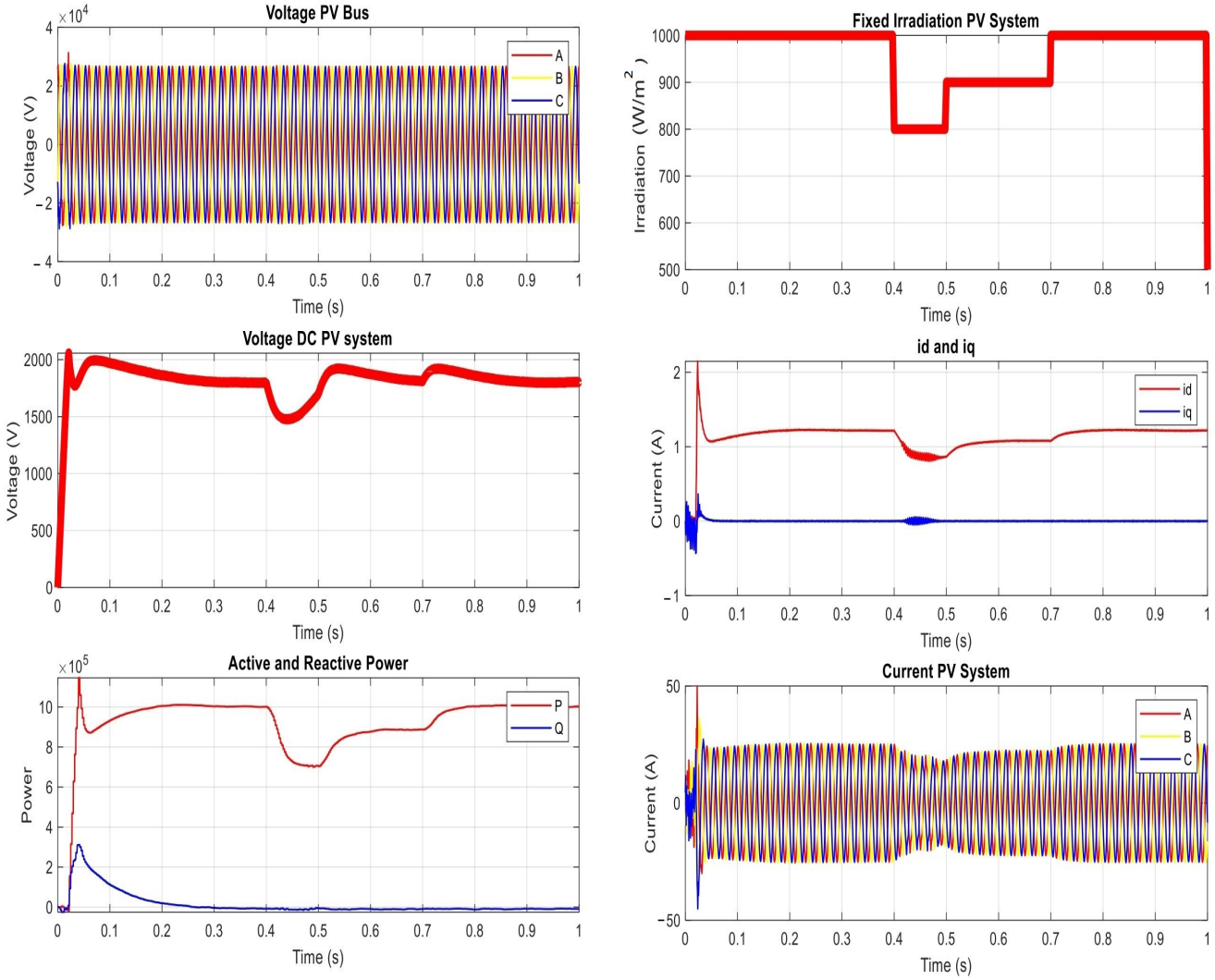

Figure 5. The results of the proposed power network under normal operation conditions with different levels of irradiation.

4.2. Results of Cyber Threats on Power Protection System (OCR)

The implementation of adaptive protection OCR schemes introduces challenges, particularly in terms of addressing communication failures and cyber threats. Consequently, any blocking or delay in the relay's response can have profound implications for grid stability. In this section, we focus on three primary cyber-attack vectors targeting the protection system illustrated in Figure 2.

- Manipulating Group Settings:

The attacker's strategy includes limiting the ability of adaptive OCR to change their group settings using FDI. In this scenario, a physical three-phase fault is applied on the low-voltage side of the transformer (T14) at time 0.5 s, as shown in Figure 6. The attacker changes the group setting of adaptive OCRs, at 0.67 s, by modifying the group setting for the primary relay (OCR4) and backup relays (OCR11 and OCR12) by activating first the group setting of backup relays. For islanding grid operation mode, this caused a drop in the PCC voltage with a high ripple, and the current from the PV system increased significantly, as shown in Figure 6. The system's dependence on the PV system caused a sudden rise in the DC voltage, leading to high ripple effects. These fluctuations were also observed in the current I_d and I_q, and active and reactive power curves. Such deviations will lead the remaining protection devices to the disconnection of the entire system.

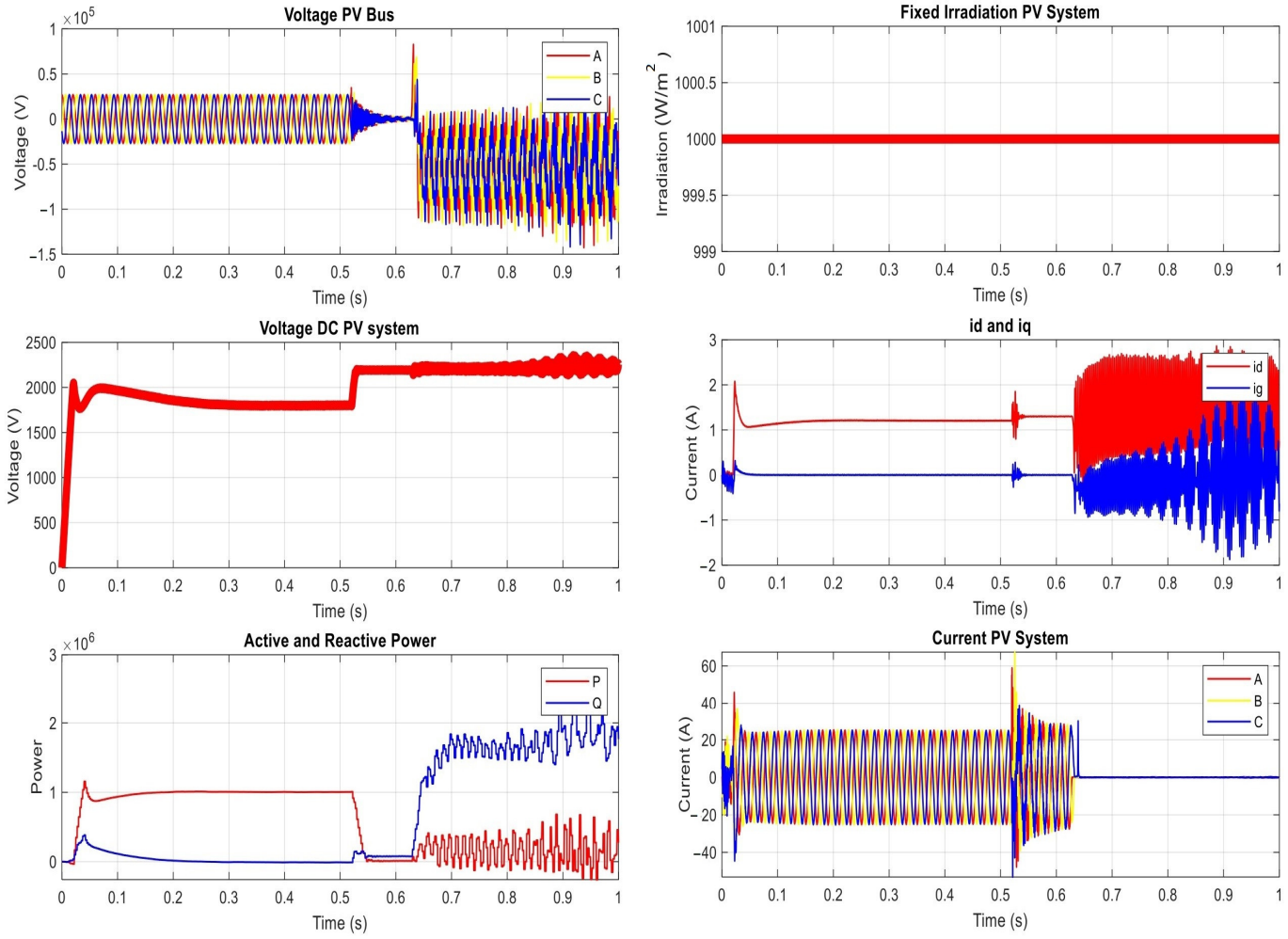

Figure 6. The results of the proposed power network under manipulating group settings attack on OCR.

- Delaying Fault Messaging

The attacker's objective is to introduce delays in the communication between the OCR and circuit breaker after detecting the physical fault, utilizing a Man-in-the-Middle (MITM) attack. This scenario can result in grid instability, as the system loses its ability to respond promptly to any detected fault, as shown in Figure 7. In this scenario, a physical three-phase fault is applied on the low-voltage side of the transformer (T14), at time 0.5 s. The attacker delays the tripping message from adaptive OCRs to reach the circuit breaker to clear the fault for around 0.3 s. This resulted in a high ripple of active and reactive power and the current from the PV system before clearing the fault, as shown in Figure 7, which will lead the remaining protection devices to disconnect from the PV system and operate the grid using only the utility source.

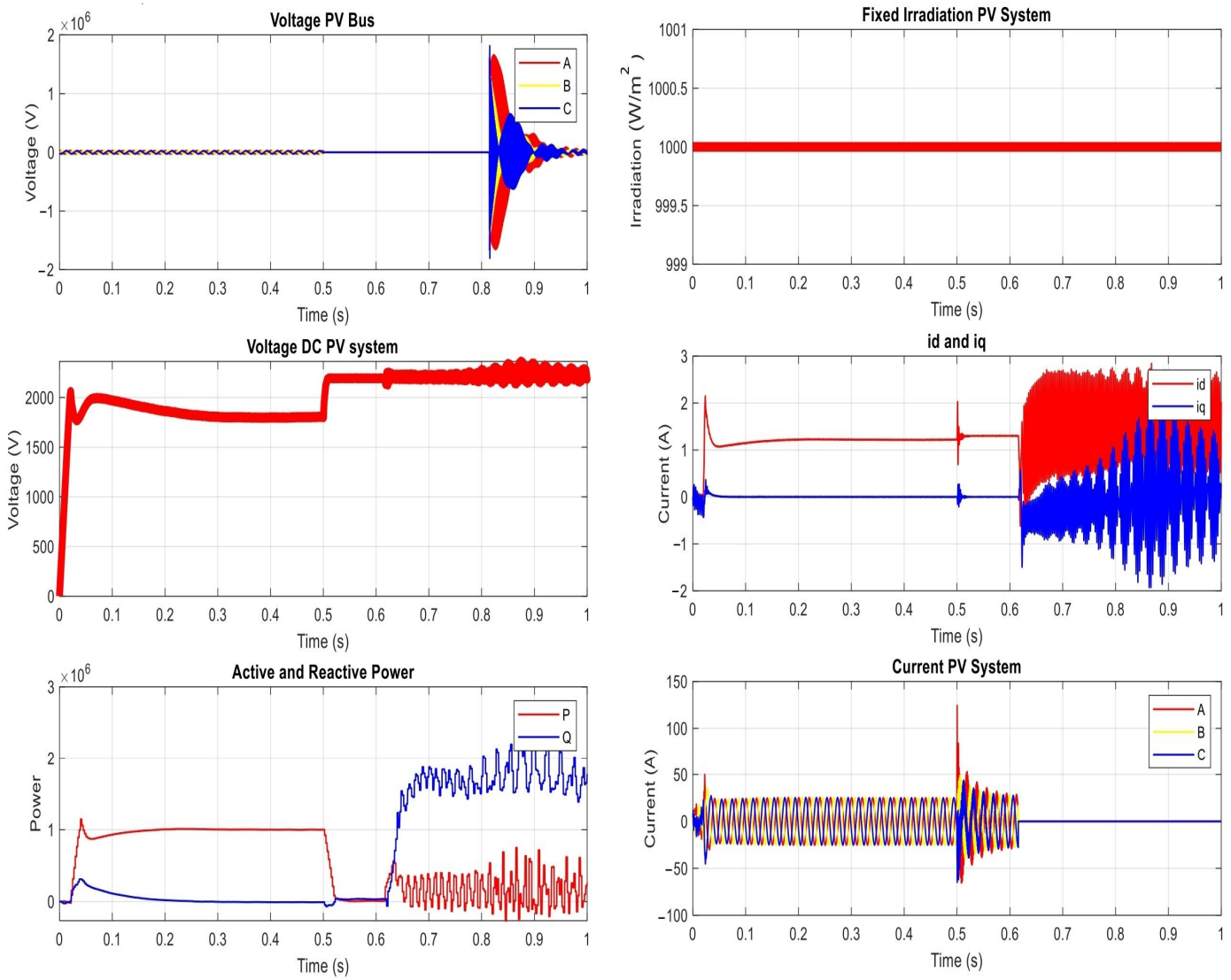

Figure 7. The results of the proposed power network under delaying fault messaging attack on transformer side.

In another case, the attacker intercepts and blocks physical fault messages originating from the OCR at the PV farm (OCR10), as shown in Figure 2. By delaying the transmission of critical fault information to the circuit breaker, the attacker seeks to create a blind spot in grid protection through a combination of Man-in-the-Middle (MIMT) and drop attacks. In this scenario, a physical three-phase fault is applied on the PV farm side of the transformer (T15), at time 0.5 s. The attacker delays the tripping message from adaptive OCRs to reach the circuit breaker to clear the fault for around 0.3 s, and during this period, the current reaches a very high level of 5000 A. This caused a power of the total PV systems equal to zero, as shown in Figure 8. The system's dependence on the PV system caused a sudden rise in the DC voltage, leading to high ripple effects. These fluctuations were also observed in the current I_d and I_q during the delay period.

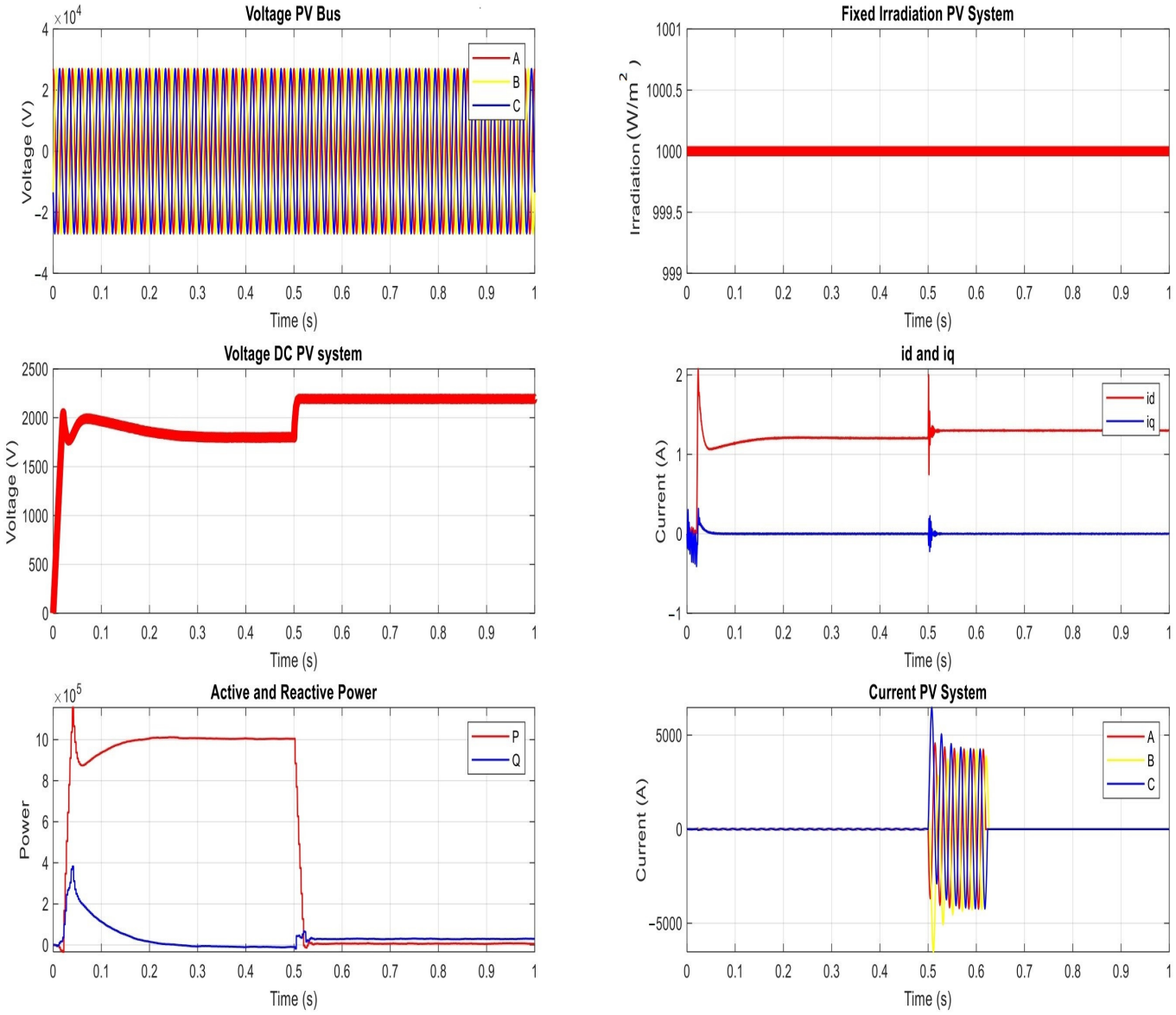

Figure 8. The results of the proposed power network under delaying fault messaging attack on PV farm side.

4.3. Results of Cyber Threats on the Smart PV Inverters

Figure 3 shows that the active and reactive power (P_{grid},Q_{grid}) are calculated and fed to the controller. This controller, as the power controller, aims to regulate the output power of the PV system by controlling the smart inverter by selecting the output active power (P) and the reactive power (Q). In the normal operation condition, the Q from the PV inverter will be zero, as shown in Figures 4 and 5. In the case of drop voltage, the inverter will feed the grid with limited reactive power to maintain the voltage level. In our study, we examine four main attack vectors against this smart inverter control system by feeding the grid reactive power during the normal operation condition. In this investigation, the operational performance of the PV system and the power grid are evaluated under normal operating conditions under a control attack targeting the control of the inverter as follows:

- Continuous Pulse Signal Attack

The attacker's strategy involves attacking the ability of the PV inverter by limiting the reactive power. In this scenario, the control signal of feeding Q to the grid will take a pulse signal shape, as shown in Figure 9. The pulse duration will be too short (10 pulses within 0.1 s). This firstly leads to an increase in the current at the source bus; however, the OCR was

not able to detect the attack and disconnect the power. In Figure 10, the supplied reactive power to the system was 2 MW, at 0.5 s. The current of the PV system experienced a high level of ripple and harmonic distortion, with peak values of approximately 50 A. The DC voltage curve similarly displayed significant distortion caused by the attack. Because the attack signal was not continuous, the protection system did not recognize the irregularity and thus failed to take any action. This absence of action in the face of abnormal power levels resulted in a significant increase in harmonic levels within the current of the PV system and increased losses.

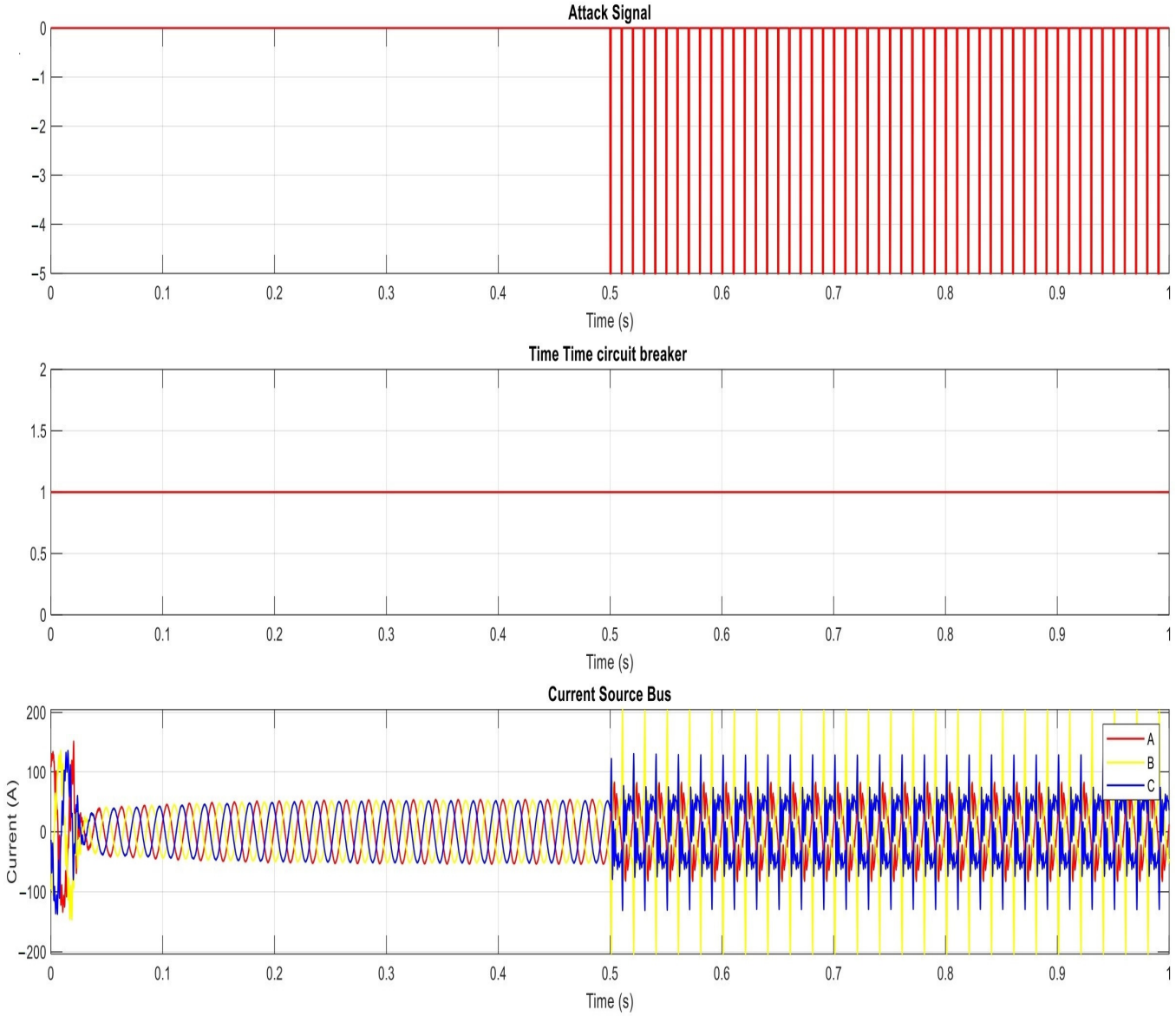

Figure 9. The continuous pulse signal attack on PV inverters.

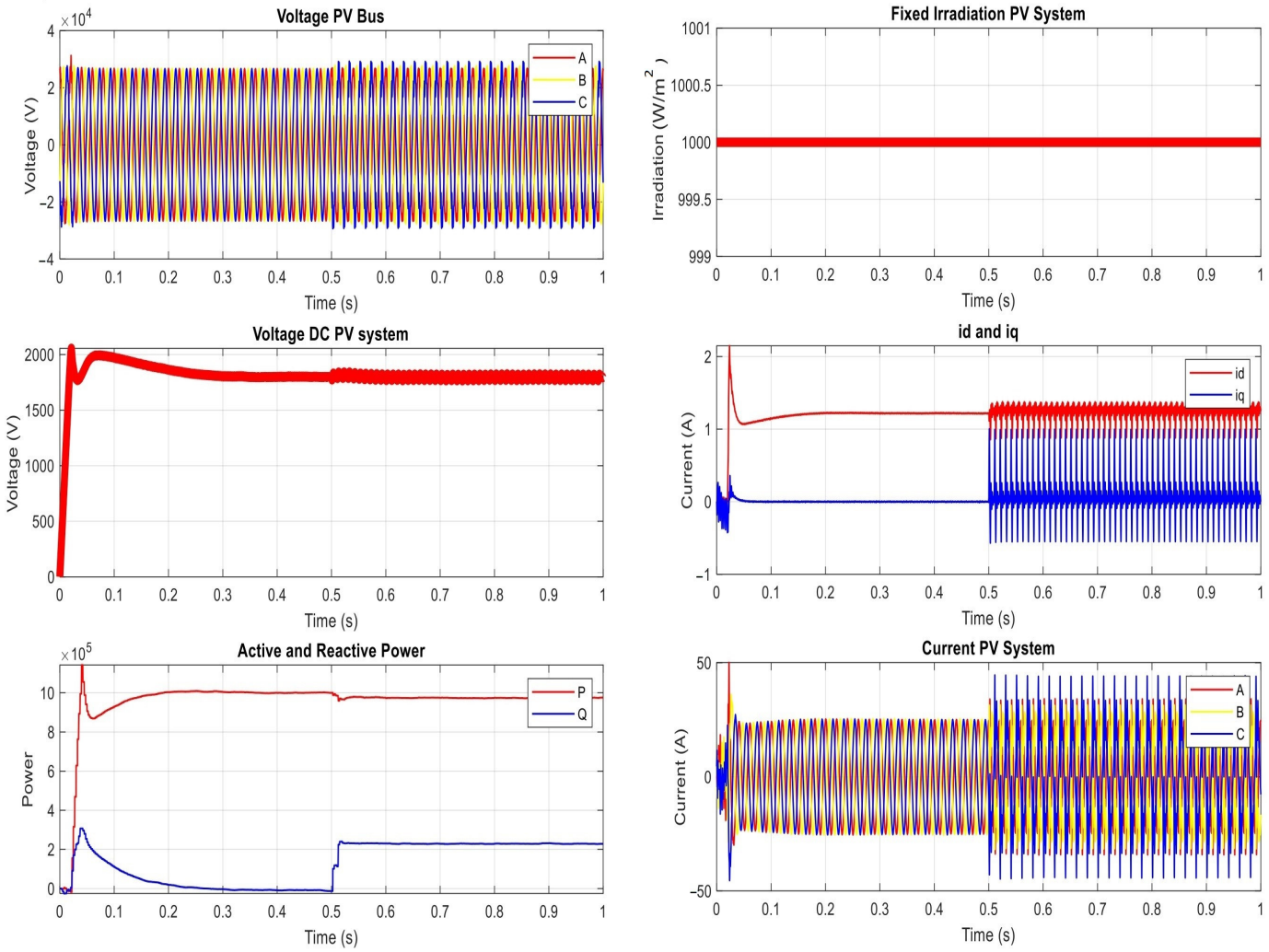

Figure 10. The results of the proposed power network under continuous pulse signal attack on PV inverters.

- Scaling Signal Attack

The technique used by the attacker involves affecting the functionality of the Photovoltaic (PV) inverter in terms of its ability to effectively control reactive power. In this particular situation, the control signal responsible for regulating the injection of reactive power into the grid displays a scaling signal waveform, as seen in Figure 11. The signal duration is significantly increased compared to pulse signal control, consisting of 1 pulse within a time range of 0.1 s. This phenomenon results in a subsequent rise in the current at the source bus. Here, the OCR was able to detect the fault and react on tripping the fault at the PV farm side at 0.65 s, as shown in Figure 11. During the initial phase of the attack (0.5 to 0.6 s), there was an increase in the current of the PV system, the system maintained overall stability. However, during the second phase of the attack when the reactive power signal dropped to -7, significant effects on the current were raised, as shown in Figures 11 and 12. The DC voltage of the PV system suffered from significant drops and fluctuations, with values dropping to 1400 V, as shown in Figure 12. These drops were accompanied by a sharp increase in the current at the source bus. As a result, the protection system disconnected the connection to the utility, leaving the system reliant only on the PV, ultimately rendering the system unstable.

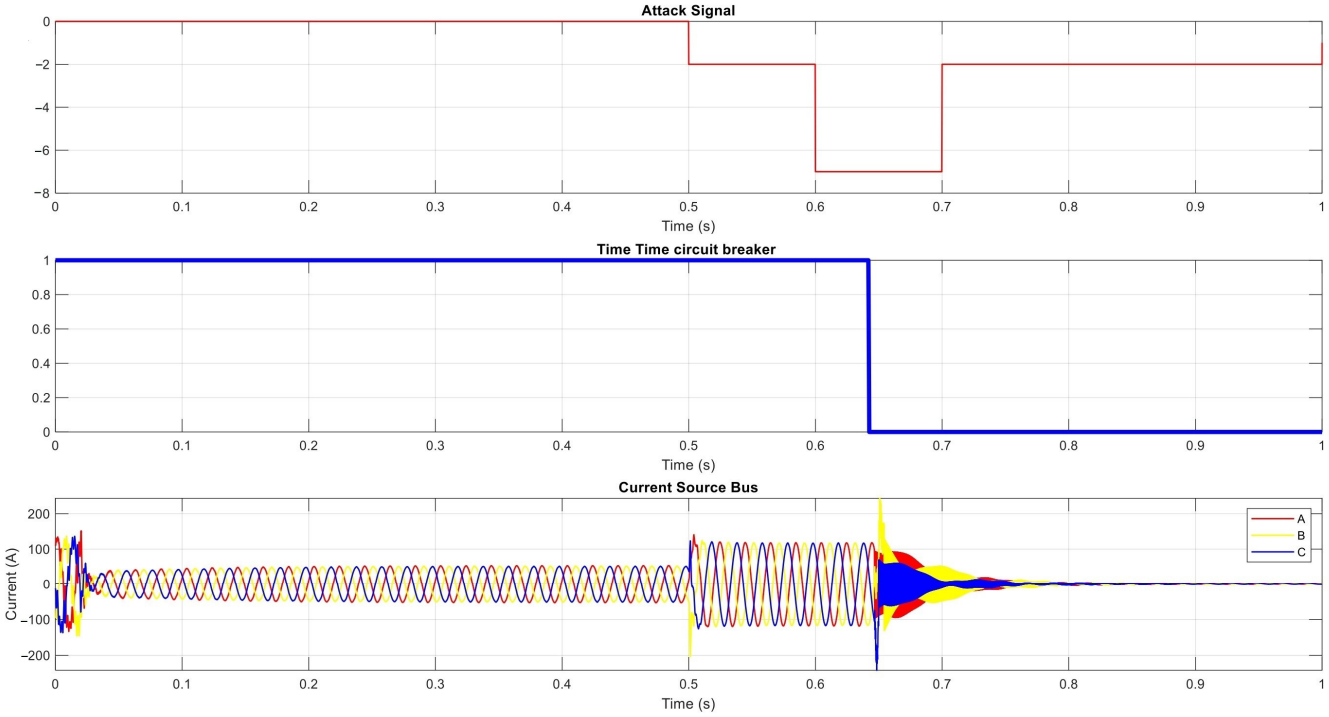

Figure 11. The scaling signal on PV inverters.

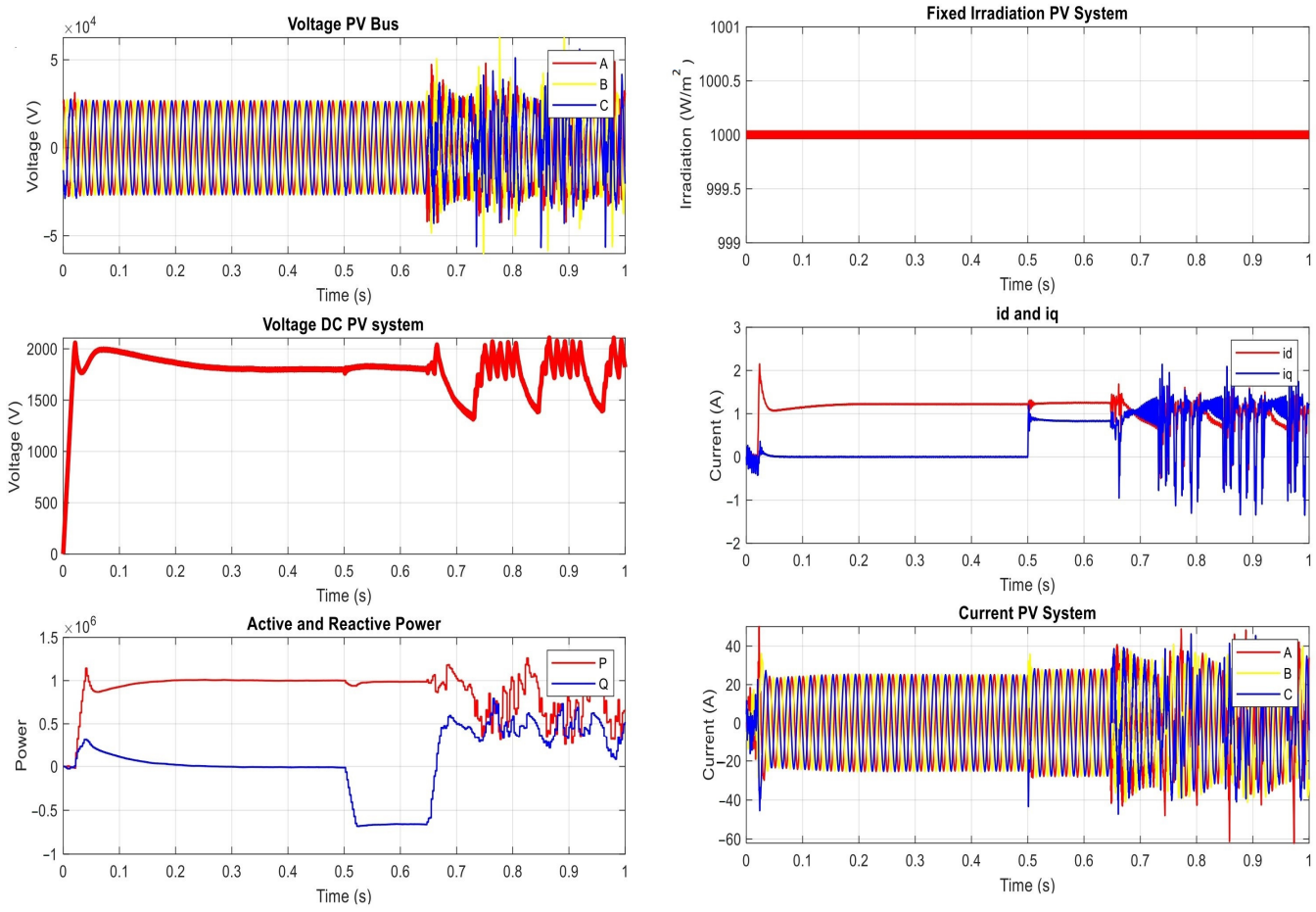

Figure 12. The results of the proposed power network under scaling signal on PV inverters.

- Sine Signal Attack

The attacker targets the functionality of the PV inverter control. In this scenario, the control signal responsible for modulating the injection of reactive power into the grid takes the form of a sine signal waveform with a sinusoidal pattern oscillating between peaks of 5 and −5, as illustrated in Figure 13. The signal duration is significantly extended compared to the pulse signal but also shorter than the scale signal. Therefore, the OCR takes more time to react and disconnect the fault at 0.7 s compared to the scale signal at 0.65 s. In the initial phase of the attack (0.5 to 0.7 s), there was a noticeable increase in the current of the PV system and a high ripple at DC voltage, P and Q, as shown in Figure 14. Consequently, the protection system disconnected the PV connection to the utility, leaving the system reliant on the utility. At 0.7 s, the protection system disconnected the utility. Upon this, the active power of the PV system dropped from its pre-attack value of 1 MW to around 0.5 MW. The entire PV system became unstable due to the attack's impact.

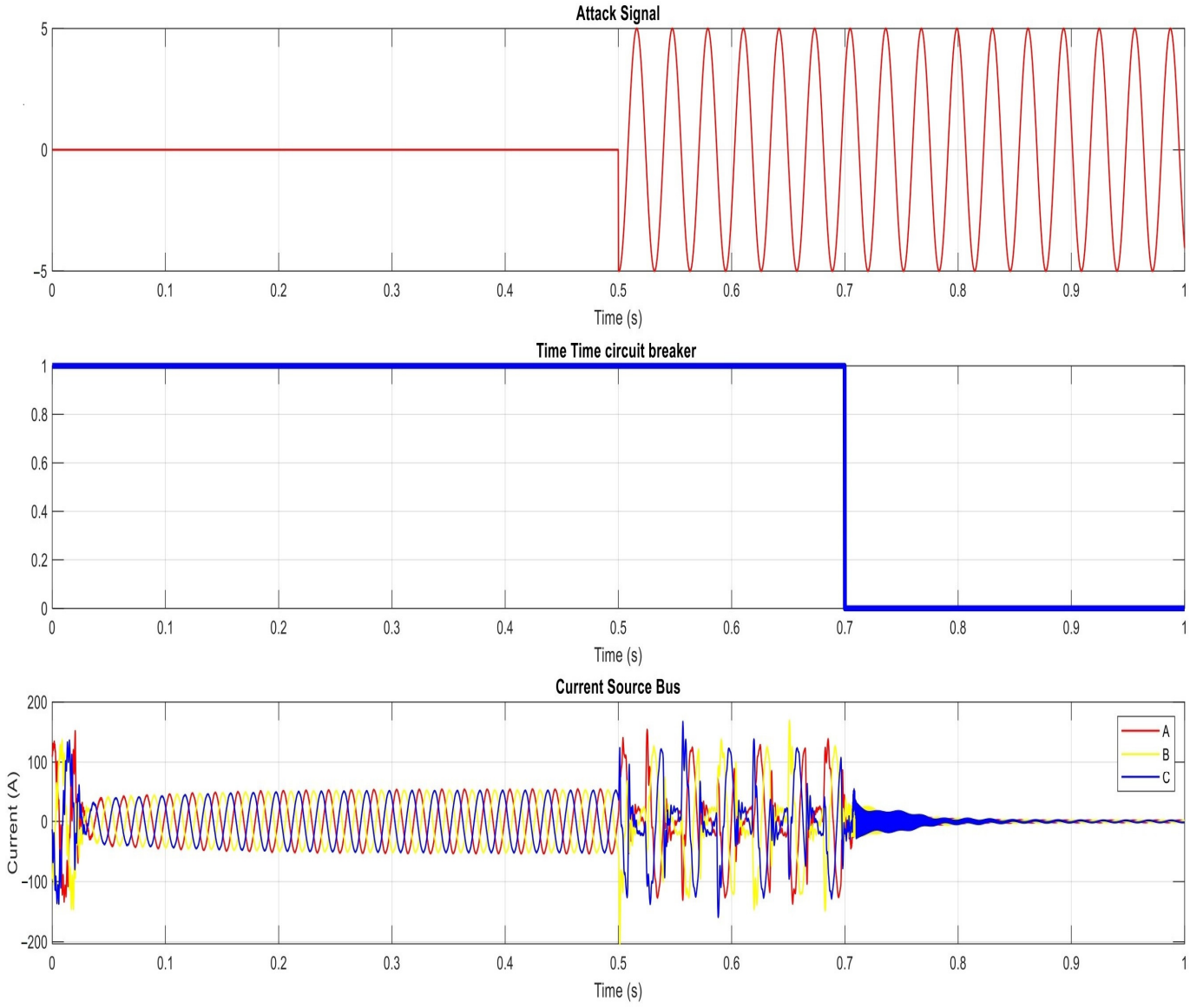

Figure 13. The sine signal attack on PV inverters.

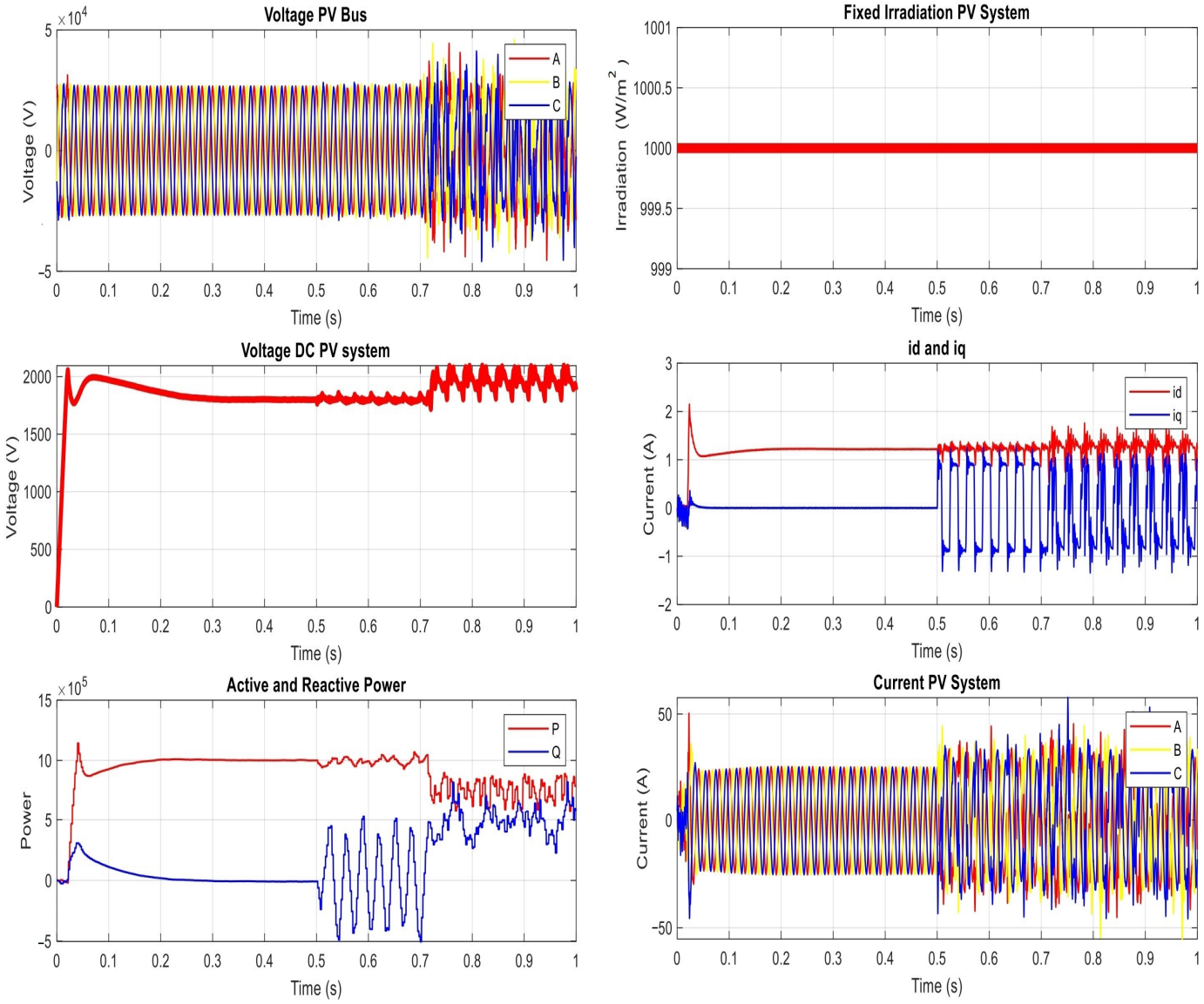

Figure 14. The results of the proposed power network under sine signal attack on PV inverters.

- Ramp Signal Attack

Ramp signal attack refers to the control signal that regulates the modulation of reactive power injection into the grid and takes the shape of a ramp waveform signal. This waveform shows a continuous drop from 0 to −5, as represented in Figure 15. As a result, the OCRs detect the fault at 0.65 s and isolates the PV system with a faster reaction in comparison to the response time of the sine signal, which needs 0.7 s, when it comes to detecting and disconnecting a problem. During the preliminary stage (0.5 to 0.65 s), there was an increase in the current of the PV system, accompanied by significant fluctuations in the DC voltage, power (P), and reactive power (Q), as seen in Figure 16. Following this, the protective system promptly disconnected the Photovoltaic (PV) connection from the utility, resulting in the system becoming totally dependent on the utility.

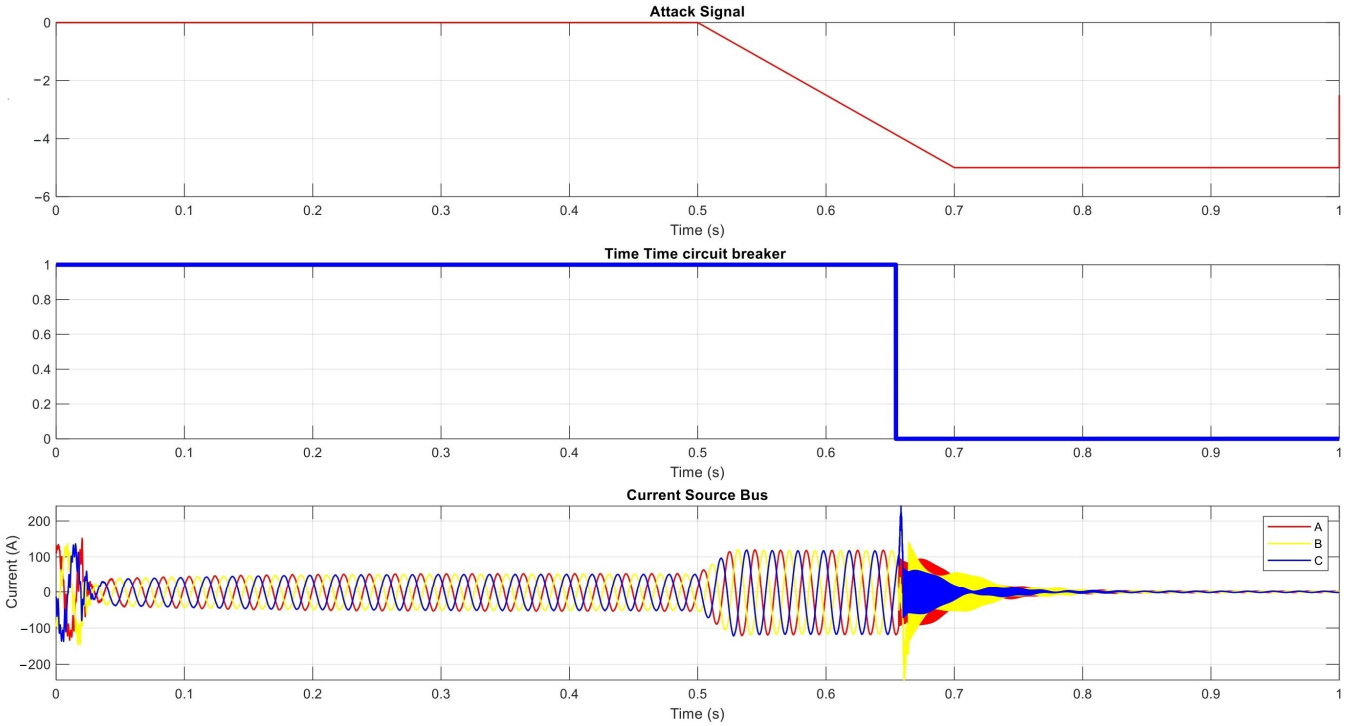

Figure 15. The ramp signal attack on PV inverters.

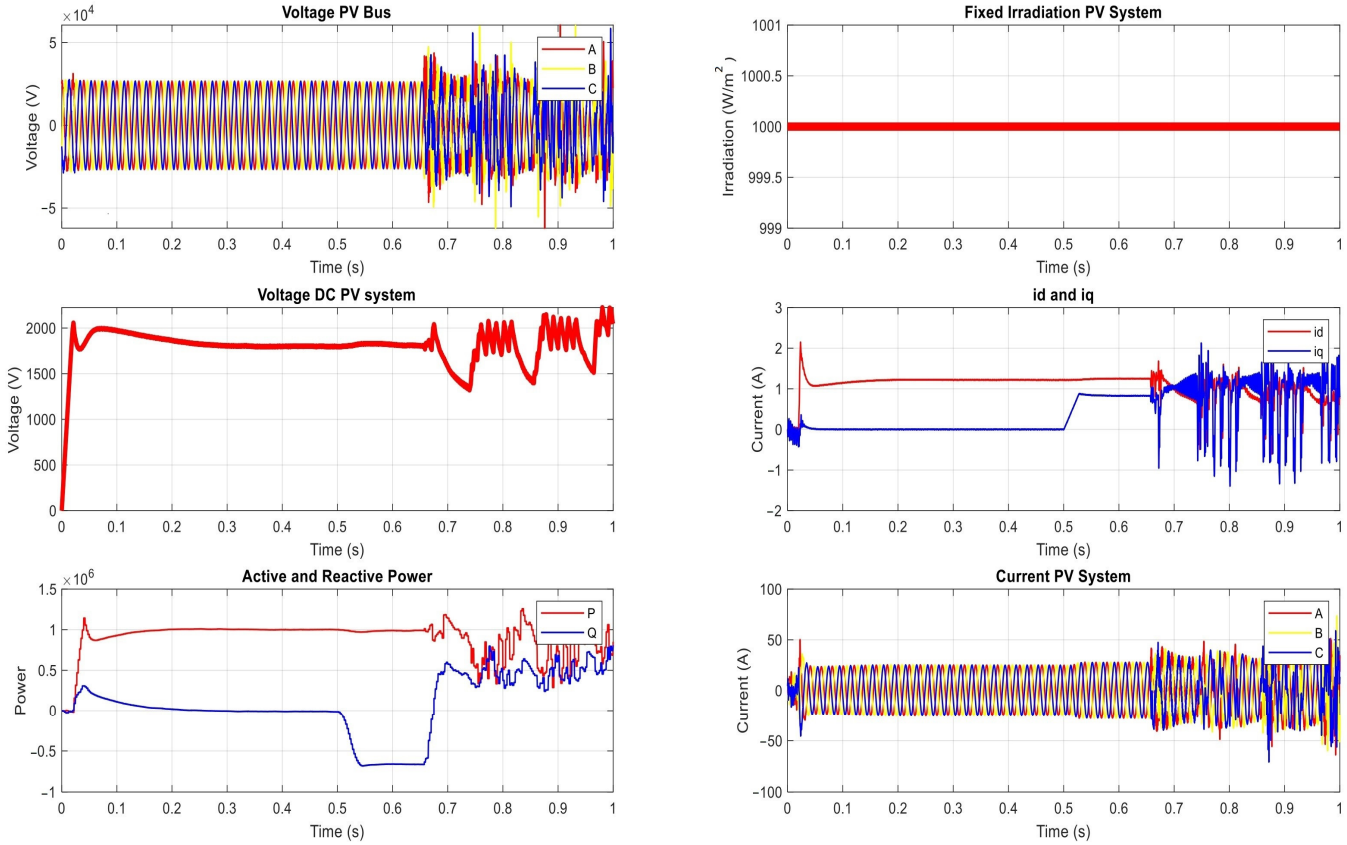

Figure 16. The results of the proposed power network under ramp signal attack on PV inverters.

4.4. Discussion

In general, this paper presents substantial results and contributions in the areas of power system protection, smart inverters, and cyber resilience. As discussed in Section 1, a

limited number of studies have examined both protection and PV control models under a cyber attack. Therefore, this study takes into consideration the research gaps that have been discovered in the current literature, as shown in Table 1. Section 4 provides a comprehensive analysis of the consequences of various cyber assaults, such as FDI, DOS, and MITM, on smart PV inverter systems and advanced OCR systems. This evaluation is carried out in line with the IEC61850 [23] and GOOSE [24] protocols, aiming to identify possible vulnerabilities and weaknesses in smart and modern power systems. In addition, the study examines the transient behavior of intelligent PV inverter and OCR systems when subjected to a cyber attack. This has been provided through a thorough evaluation of the system's interaction during different types of cyber-attack events. In addition, to enhance the existing knowledge in the field by creating an accurate model of a power network, the EMTP is used. This modeling allows for the investigation of temporary occurrences and timeframes under several grid operating scenarios, including normal operation, continuous operation with decreases in irradiation, and different cyber attacks at smart inverters and OCR under fault events, as shown in Section 4 and summarized in Table 5.

Table 5. The results of the proposed power network under manipulating group settings attack on OCR, sine, and ramp signal attack on PV inverters.

The Results of the Proposed Power Network under Manipulating Group Settings Attack on OCR			
	t ∈ [0, 0.5) s	t ∈ [0.5, 0.64) s	t ∈ [0.64, 1) s
Irradiation	1000	1000	1000
DC Voltage	1800	2192	random
Active Power	1 MW	Zero	random
Reactive power	Zero	77.4	random
Current PV(AC)	24.6	58.2	zero
Voltage (AC)	25.94 kV	Zero	random
Id	1.2	1.8	random
Iq	Zero	Zero	random
The results of the proposed power network under sine signal attack on PV inverters			
	t ∈ [0, 0.5) s	t ∈ [0.5, 0.64) s	t ∈ [0.64, 1) s
DC Voltage	1800	[1780–1860]	[1800–2100]
Active Power	1 MW	[9.5–10.5] MW	[6–8.5] MW
Reactive power	ZERO	$[(-5)–5] \times 10^5$	$[3–5] \times 10^5$
Current PV(AC)	25	35	35
Voltage (AC)	26 kV	45 kV	45 kV
Id	1.2	[1–1.4]	[0.6–1.6]
Iq	Zero	−1.2/1.2	−1.2/1.2
The results of the proposed power network under ramp signal attack on PV inverters			
	t ∈ [0, 0.5) s	t ∈ [0.5, 0.64) s	t ∈ [0.64, 1) s
DC Voltage	1800 V	2029	Unstable
Active Power	1 MW	1 MW	Unstable
Reactive power	Zero	−0.66 MW	Unstable
Current PV(AC) 1 Ph	25.6 A	37.52 A	52 A
Voltage (AC)	26.5 kv	Unstable	unstable
Id	1.2 A	1.2 A	Unstable
Iq	Zero	0.5 A	Unstable

The control signal attacks (pulse, sine, ramp, and scale attacks), as shown in Section 4.3, involve disrupting the stability of the grid by chaining the characteristic of the reactive power control, volt–var control. In the IEEE-1547-2020 standard [5,15], the volt–var curve is utilized to manage the grid's operating voltage by introducing or absorbing reactive power up to 44% of the rated active power of the inverter. Unwanted flow of reactive power in the system, resulting in under- or over-voltages, may lead to technical challenges and economic losses. These issues heighten the risk of failures in circuit equipment. In the case of inverters prioritizing reactive power based on the IEEE-1547 standard, modification attacks that involve injecting or absorbing excessive reactive power can lead to active power curtailment, causing financial losses in terms of active power revenue for the system owner [28,29]. A high level of reactive power in the system can cause voltage fluctuations, which can result in technical difficulties and financial losses. These concerns increase the possibility of failures in circuit equipment. Through our results and the utilization of the OCR protection currently used in the power network, the majority of cyber attacks at the smart inverter level did not impact the OCR protection working principle, except in the case of the pulse attack signal. This is due to the signal duration, which is too short (10 pulses within 0.1 s). Therefore, in the future, a proposed solution may be introduced that does not rely on the current level but also incorporates voltage and harmonics. According to the results in Section 4.3 and the implementation of OCR protection in the power network, most cyber-attack-targeting smart inverters did not affect the functioning of the OCR protection, except in the event of a pulse attack signal. Therefore, a coordinated cyber-attack scenario targeted multiple components (smart inverter and OCR) simultaneously. In this coordinated attack scenario, the ramp signal attack is used to change the reactive power level at the smart inverter, and the delay attack is used to delay the command communication between the OCR and circuit breaker after detecting the physical fault, as shown in Figure 17. The reactive power to the system was −0.6 MW, at 0.5 s. The current of the PV system increased and the current at the source bus achieved 100 A. Because of the coordinated attack, the protection system did not recognize the fault and thus failed to take action, as seen in Figure 18.

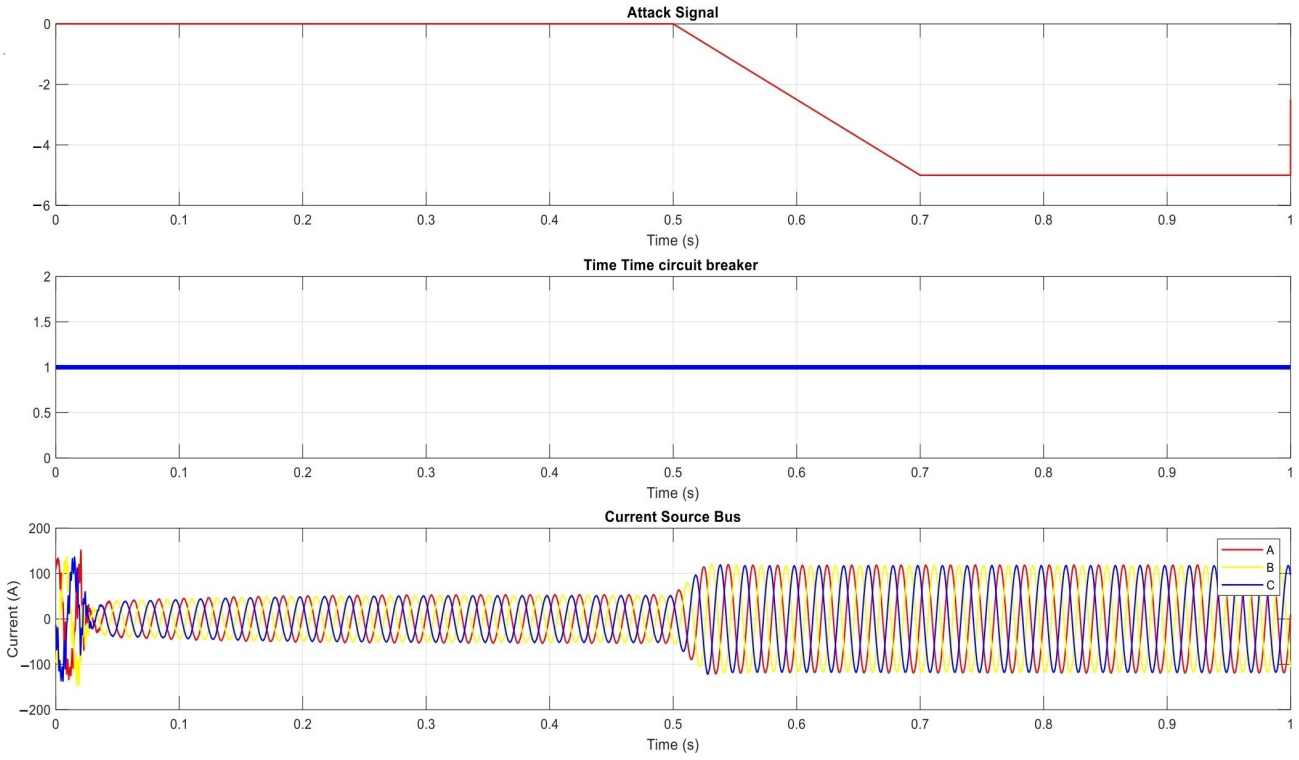

Figure 17. The ramp signal attack on PV inverters and circuit breaker during fault condition.

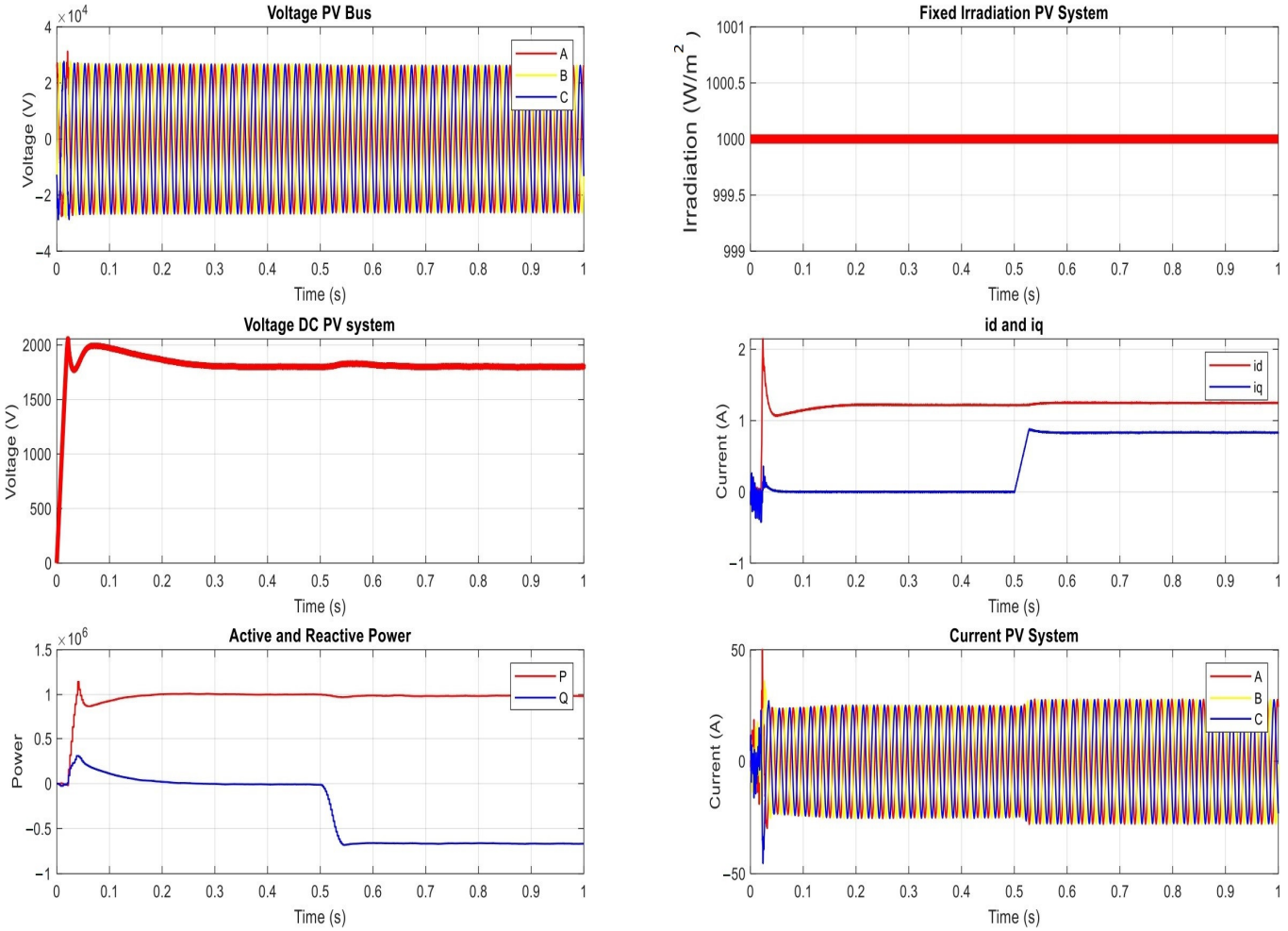

Figure 18. The results of the proposed power network under ramp signal attack and circuit breaker on PV inverters.

Overall, the results of this study, which utilized a practical network (real network model, as presented in Section 3) and simulated traditional faults and cyber-physical attacks using the widely used EMTP tool while also taking into account OCR characterizes based on IEC255-3 standards [2,29] and the IEEE-1547-2018 standards [5,15] for smart inverters, offer significant insights. These standards are considered standards for all types of inverters and OCR. Therefore, the findings of this work can be generalized to real-world scenarios. One potential opportunity for study involves investigating the application of machine learning methods to enhance the identification of cyber attacks, particularly in the domain of power systems. Utilizing machine learning algorithms may greatly enhance cybersecurity against advanced attacks, offering a stronger protection mechanism. Another potential path for future research is the development and application of a real-time Hardware-in-the-Loop (HIL) system that is combined. This technique provides a more realistic and dynamic setting for testing and assessing the resilience of power systems against cyber threats in real-time scenarios. The paper can contribute to expanding the field of power system security and cyber resilience by addressing these future research objectives. This will eventually enhance the dependability and stability of current power grids.

5. Conclusions

The focus of this study is on the increasing difficulties associated with the incorporation of DERs and communication networks, namely in the field of smart inverter control and protection. The study highlights the significant issue of cyber attacks and their possible effects on grid stability in the context of the growing development of grid-connected PV

systems. In addition, this work explores the consequences of cyber attacks when specifically targeting components of smart grids, focusing particularly on smart PV inverters and OCR. A complete investigation of grid modeling and transient impacts under several cyber-attack scenarios was carried out using the EMTP.

The research findings provide insight into the relationship between vulnerabilities in inverters and relays, providing a clearer understanding of the extensive consequences that attacking one component can have on the other. Moreover, the objective of this study is to evaluate the wider impact of cyber attacks on the overall efficiency and reliability of grid-connected PV systems in a smart grid. For example, in the attack on the PV inverters employing a pulse signal with a short duration of 0.1 s, the OCR failed to detect and disconnect the power. This led to increased current, reaching 50 A, significant harmonic distortion, and high power losses due to the protection system's inability to recognize and respond to the irregular attack signal. It provides a substantial contribution to the understanding of cybersecurity issues that are present in grid-connected PV systems. This highlights the critical importance of implementing advanced protection measures and resilience strategies to effectively over modern and dynamic smart grid systems. The ongoing development of DERs and communication networks requires a comprehensive understanding of cyber threats. Furthermore, this study is essential in maintaining the long-term reliability and stability of modern power networks.

Author Contributions: Conceptualization, F.A., A.I. and N.E.-N.; methodology, S.A.G., F.A., M.A. and N.E.-N.; software, A.I., F.A. and A.M.H.; validation all authors; formal analysis, F.A., A.A., N.E.-N. and A.M.H.; investigation, F.A., A.I. and N.E.-N.; resources, all authors; data curation, all authors; writing—original draft preparation, F.A., A.I. and S.A.G.; writing—review and editing, all authors; visualization, all authors; supervision, all authors; project administration, A.I., F.A. and A.M.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by funding from the Scientific Research and Innovation Support Fund, Ministry of Higher Education Scientific Research, the Hashemite Kingdom of Jordan, under grant number (ENE/1/02/2022), https://cyberssgridhu.github.io/index.html (11 November 2023).

Data Availability Statement: Derived data supporting the findings of this study are available from the corresponding author on request.

Acknowledgments: We would like to thank the Hashemite University (Renewable Energy Center) for their support in publishing this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Holderbaum, W.; Alasali, F.; Sinha, A. *Energy Forecasting and Control Methods for Energy Storage Systems in Distribution Networks, Predictive Modelling and Control Techniques*, 1st ed.; Springer: Cham, Switzerland, 2023.
2. Brahma, S.M.; Girgis, A.A. Development of adaptive protection scheme for distribution systems with high penetration of distributed generation. *IEEE Trans. Power Deliv.* **2004**, *19*, 56–63. [CrossRef]
3. Ahmed, A.; Krishnan, V.V.; Foroutan, S.A.; Touhiduzzaman, M.; Rublein, C.; Srivastava, A.; Suresh, S. Cyber physical security analytics for anomalies in transmission protection systems. *IEEE Trans. Ind. Appl.* **2019**, *55*, 6313–6323. [CrossRef]
4. Olowu, T.O.; Dharmasena, S.; Jafari, H.; Sarwat, A. Investigation of false data injection attacks on smart inverter settings. In Proceedings of the 2020 IEEE CyberPELS (CyberPELS), Miami, FL, USA, 13 October 2020; pp. 1–6.
5. Peng, S.; Liu, M.; Zuo, K.; Tan, W.; Deng, R. Stealthy Data Integrity Attacks Against Grid-tied Photovoltaic Systems. In Proceedings of the 2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS), Wuhan, China, 8–11 May 2023; pp. 1–7.
6. Yousefi kia, M.; Saniei, M.; Seifossadat, S.G. A novel cyber-attack modelling and detection in overcurrent protection relays based on wavelet signature analysis. *IET Gener. Transm. Distrib.* **2023**, *17*, 1585–1600. [CrossRef]
7. Zhou, J.; Feng, C.; Su, Q.; Jiang, S.; Fan, Z.; Ruan, J.; Sun, S.; Hu, L. The Multi-Objective Optimization of Powertrain Design and Energy Management Strategy for Fuel Cell–Battery Electric Vehicle. *Sustainability* **2022**, *14*, 6320. [CrossRef]
8. Lu, D.; Yi, F.; Hu, D.; Li, J.; Yang, Q.; Wang, J. Online optimization of energy management strategy for FCV control parameters considering dual power source lifespan decay synergy. *Appl. Energy* **2023**, *348*, 121516. [CrossRef]
9. Nasirian, V.; Shafiee, Q.; Guerrero, J.M.; Lewis, F.L.; Davoudi, A. Droop-Free Distributed Control for AC Microgrids. *IEEE Trans. Power Electron.* **2016**, *31*, 1600–1617. [CrossRef]

10. Rosero, C.X.; Velasco, M.; Martí, P.; Camacho, A.; Miret, J.; Castilla, M. Active Power Sharing and Frequency Regulation in Droop-Free Control for Islanded Microgrids Under Electrical and Communication Failures. *IEEE Trans. Ind. Electron.* **2020**, *67*, 6461–6472. [CrossRef]
11. Mahmud, M.A.; Hossain, M.J.; Pota, H.R.; Oo, A.M.T. Robust Nonlinear Distributed Controller Design for Active and Reactive Power Sharing in Islanded Microgrids. *IEEE Trans. Energy Convers.* **2014**, *29*, 893–903. [CrossRef]
12. Rey, J.M.; Vergara Barrios, P.; Castilla, M.; Camacho, A.; Velasco, M.; Martí, P. Droop-free hierarchical control strategy for inverter-based AC microgrids. *IET Power Electron.* **2020**, *13*, 1403–1415. [CrossRef]
13. Sowa, I.; Monti, A. On Dynamics of Communication-Based Distributed Consensus Control in Islanded Microgrids. In Proceedings of the 2022 International Conference on Smart Energy Systems and Technologies (SEST), Eindhoven, The Netherlands, 5–7 September 2022.
14. Majumder, S.; Vosughi, A.; Mustafa, H.; Warner, T.; Srivasava, A. On the Cyber-Physical Needs of DER-based Voltage Control/Optimization Algorithms in Active Distribution Network. *IEEE Access* **2022**, *10*, 64397–64429. [CrossRef]
15. Liu, X.; Li, H. Data-driven Cyberphysical Anomaly Detection for Microgrids with GFM Inverters. *IEEE Open J. Power Electron.* **2023**, *4*, 498–511. [CrossRef]
16. Kaewnukultorn, T.; Sepúlveda-Mora, S.B.; Broadwater, R.; Zhu, D.; Tsoutsos, N.G.; Hegedus, S. Smart PV Inverter Cyberattack Detection using Hardware-in-the-Loop Test Facility. *IEEE Access* **2023**, *99*, 90766–90779. [CrossRef]
17. Bamigbade, A.; Dvorkin, Y.; Karri, R. Cyberattack on phase-locked loops in inverter-based energy resources. *IEEE Trans. Smart Grid* **2023**, 1. [CrossRef]
18. Zhang, J.; Guo, L.; Ye, J.; Giani, A.; Elasser, A.; Song, W.; Mantooth, H.A. Machine Learning-based Cyber-attack Detection in Photovoltaic Farms. *IEEE Open J. Power Electron.* **2023**, *4*, 653–673. [CrossRef]
19. Piesciorovsky, E.C.; Hahn, G.; Hink, R.B.; Werth, A.; Lee, A. Electrical substation grid testbed for DLT applications of electrical fault detection, power quality monitoring, DERs use cases and cyber-events. *Energy Rep.* **2023**, *10*, 1099–1115. [CrossRef]
20. Aftab, M.A.; Chawla, A.; Vergara, P.P.; Ahmed, S.; Konstantinou, C. Volt/VAR Optimization in the Presence of Attacks: A Real-Time Co-Simulation Study. In Proceedings of the IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Aachen, Germany, 25–28 October 2021.
21. Rajaee, M.; Mazlumi, K. Multi-Agent Distributed Deep Learning Algorithm to Detect Cyber-Attacks in Distance Relays. *IEEE Access* **2023**, *11*, 10842–10849. [CrossRef]
22. Jadidi, S.; Badihi, H.; Zhang, Y. Design of an intelligent hybrid diagnosis scheme for cyber-physical PV systems at the microgrid level. *Int. J. Electr. Power Energy Syst.* **2023**, *150*, 109062. [CrossRef]
23. Sowa, I.; Monti, A. Distributed Consensus Control Supported by High Reporting Rate Meters in Inverter-Based Cyber-Physical Microgrids. *IEEE Access* **2023**, *11*, 48305–48321. [CrossRef]
24. Elrawy, M.F.; Tekki, E.; Hadjidemetriou, L.; Laoudias, C.; Michael, M.K. Protection and Communication Model of Intelligent Electronic Devices to Investigate Security Threats. In Proceedings of the 2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 16–19 January 2023; pp. 1–5.
25. Zaki, M.; El Sehiemy, R.; Megahed, T.; Asano, T.; Abdelkader, S. A proposed fault identification-based fuzzy approach for active distribution networks with photovoltaic systems. *Measurement* **2023**, *223*, 113678. [CrossRef]
26. De Oliveira-De Jesus, P.M.; Sorrentino, E. Methodology to assess performance indexes for sensitivity, selectivity, and speed of coordination of directional overcurrent protections. *Electr. Power Syst. Res.* **2022**, *213*, 108758. [CrossRef]
27. Gonzalez, R.; Aryasomyajula, V.; Ayyagari, K.; Gatsis, N.; Alamaniotis, M.; Ahmed, S. Modeling and studying the impact of dynamic reactive current limiting in grid-following inverters for distribution network protection. *Electr. Power Syst. Res.* **2023**, *224*, 109609. [CrossRef]
28. Pramanik, A.S.; Sepasi, S. Transient Behavior Analysis of Microgrids in Grid-Connected and Islanded Modes: A Comparative Study of LVRT and HVRT Capabilities. *Clean Technol.* **2023**, *5*, 1287–1303. [CrossRef]
29. Kumar, J.; Sikdar, B.; Kundur, D. Three-Phase Radial EMTP and Stealthy Attack Detector for Distribution Systems. In Proceedings of the IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), Jaipur, India, 16–19 December 2020.