

ORIGINAL RESEARCH

Open access

Impact of Cyber Attacks on Grid-Connected PV Systems: Enhancing Resilience of Inverters and Protection Systems

Priya Nambiar^{1*}, Suresh Menon¹, Kavita Pillai²

Abstract

Over the past few years, integrating Distributed Energy Resources (DERs) with advanced communication infrastructures has created major challenges for the control and protection of electrical power systems. These difficulties stem mainly from the rapid evolution of smart grids and the growing threat of cyberattacks. As grid-tied solar Photovoltaic (PV) installations—equipped with smart inverters—become more widespread, their exposure to malicious cyber activities and the resulting risks to power network stability have become a pressing issue, especially given the inverter control logic. The present study examines the outcomes of targeted cyber intrusions targeting key PV system elements, with particular attention to the inverter and the Overcurrent Protection Relay (OCR). It further analyzes how these two components interact across a range of cyber-attack conditions. Simulations are conducted using a three-phase radial Electromagnetic Transients Program (EMTP) model to represent the grid and study transient responses during various cyber intrusions. Analysis results uncover the tight coupling between weaknesses in inverters and protection relays, demonstrating how disruption of one can severely affect the performance of the other. The work also quantifies how cyber incidents degrade the efficiency and operational reliability of PV systems connected to the grid. As a concrete illustration, when PV inverters were subjected to a brief 0.1 s pulse signal attack, the OCR failed to detect the abnormality and isolate the fault. This breakdown caused pronounced harmonic distortion together with considerable active power losses, stemming directly from the protection scheme's inability to recognize and counteract the irregular disturbance. Overall, this investigation provides important new insights into cybersecurity challenges in grid-integrated solar PV installations. It underscores the urgent need to adopt stronger defensive strategies and build greater system resilience as power networks continue evolving into intelligent, interconnected smart grids.

Keywords Smart grid, Cyber threats, PV, Overcurrent relay, Intelligent inverter

*Correspondence:

Priya Nambiar

priya.nambiar@iisc.ac.in

¹ Department of Smart Grid Engineering, Faculty of Engineering, Indian Institute of Science, Bengaluru, India

² Department of Energy Optimization and Control, Faculty of Engineering, Anna University, Chennai, India

Introduction

Motivation

The share of Distributed Energy Resources (DERs) powered by renewable sources within electrical networks is steadily increasing, supported by remarkable technological advances that enable environmentally friendly and economically attractive electricity generation [1]. In response, power utilities are progressively integrating numerous intelligent

electronic devices (IEDs)—such as smart meters, inverters, and protection relays—into their infrastructure. The increasing presence of DERs has heightened reliance on communication links among IEDs, spanning both intra- and inter-substation environments. Ensuring reliable and secure functioning of today's smart power grids, therefore, demands careful management of the intricate interplay between digital intelligent devices and the underlying physical power assets [1, 2].

Within smart grid frameworks, the growing reliance on data- and communication-centric control methods has heightened cybersecurity concerns. Modern smart PV inverters rely on sophisticated power-electronic hardware—including microcontrollers, digital signal processors, and various Integrated Circuits (ICs)—leaving them open to multiple forms of cyber compromise, ranging from manipulation of data integrity to exploitation of communication channels. Additionally, delayed or missing firmware patches in large-scale PV facilities have caused erratic inverter operation, resulting in unexpected shifts in power factor, voltage instability, and other irregularities [3]. In present-day control architectures, these inverters are frequently managed remotely via SCADA platforms that use Ethernet, optical fiber, or wireless links for data exchange [4, 5]. All such communication pathways remain vulnerable to cyber compromise, potentially enabling malicious actors to assume unauthorized command over system converters and block legitimate operator intervention [6]. At the same time, protective relays—implemented as IEDs—are charged with sensing abnormal conditions and executing corrective actions via diverse protection algorithms. Failures to properly address such disturbances can result in equipment degradation or, at the very least, reduce the service life of critical grid components [5, 6]. Relay trip signals are commonly transmitted using the high-speed GOOSE protocol to enable swift backup protection response.

To date, relatively few publications have addressed the robustness of smart PV inverters and their associated protection systems when subjected to combined cyber-physical attacks, particularly grounded in realistic distribution network configurations. Moreover, existing literature reviews show that the transient dynamic behavior of power systems—specifically involving smart PV inverters and protection devices—under active cyber-attack conditions has been largely overlooked. For these reasons, the current study explores a range of cyber-physical threat scenarios targeting smart PV inverter control logic and OCR-based protection schemes, with simulations conducted using the Electromagnetic Transients Program (EMTP).

Literature review

In contemporary smart grid and advanced power network frameworks, the reliable delivery of electrical power depends heavily on effective smart energy management strategies for Distributed Energy Resources (DERs), including photovoltaic (PV) systems, fuel cell–battery hybrids, and electric vehicles [7]. Real-time enhancement of energy management within grid control configurations remains essential [8]. Consequently, the power systems sector is undergoing a profound shift driven by the adoption of cutting-edge technologies, particularly in smart PV inverters, protective mechanisms, and cyber-physical safeguards. Over recent years, scholarly investigations into the weaknesses, risks, and potential countermeasures for modern intelligent electricity infrastructures have expanded considerably. This subsection provides an in-depth survey of key studies that have analyzed the ramifications of cyber-physical threats on smart grids incorporating grid-tied PV installations.

The work by Nasirian *et al.* [9] offered a thorough overview of consensus-based control, a primary mechanism for regulating active and reactive power flows in microgrids. Their analysis demonstrated that, despite discrepancies in nodal reference values, a distributed setup can accomplish practical power distribution proportional to rated capacities. The control action is restricted to nodes with available unconstrained capacity, ultimately leading to stabilization around an average voltage that lacks direct regulation.

Rosero *et al.* [10] introduced a distributed control framework tailored for active power and frequency regulation in microgrids. They assessed system stability by evaluating critical linkages in both communication and physical domains, although cyber-layer delays were overlooked. Mahmud *et al.* [11] proposed a communication-independent distributed controller that avoids traditional droop methods, instead employing a resilient distributed approach to enable active and

reactive power sharing among subsystems featuring multiple DER units. Nevertheless, the studies by Nasirian *et al.* [9], Rosero *et al.* [10], and Mahmud *et al.* [11] did not address potential influences from communication infrastructures, cyber-layer dynamics, or convergence behavior under attack conditions. Reviews presented in Rosero *et al.* [10], Mahmud *et al.* [11], and Rey *et al.* [12] surveyed diverse PV control strategies employed in microgrids, which generally depend on communication-supported techniques combined with droop-based or droop-free operations. The analysis by Rey *et al.* [12] considered multiple communication topologies, typically assuming fixed, small-scale delays in limited network setups.

Only a handful of investigations have examined the repercussions of cyber intrusions on intelligent power networks featuring DERs, especially PV systems. Sowa and Monti [13] studied a consensus-driven control approach for islanded microgrids that accounts for interactions across cyber and physical domains. Their scheme was engineered to accommodate arbitrary electrical and communication structures with diverse properties, successfully fulfilling primary and secondary control goals within a single unified framework. The modeled cyber component was developed to integrate physical and cyber aspects, including interlayer dynamics and interconnections, while robustness was bolstered by incorporating and countering model uncertainties. Still, the implications of communication issues, cyber-layer vulnerabilities, and control convergence across varied cyber-attack profiles were not sufficiently explored. Majumder *et al.* [14] categorized components across the communication, physical, and cyber domains, focusing primarily on cataloging different cyber threats targeting those layers. In a separate effort, Liu and Li [15] evaluated cyber-physical risks in a microgrid with grid-forming inverters operating under low short-circuit conditions. Yet, their examination omitted diverse attack types, realistic grid parameters, and considerations of protective equipment.

Moreover, incorporating inverters into distribution systems can alter fault-propagation patterns and increase fault currents, potentially leading to erroneous operation of protection devices, such as the Overcurrent Relay (OCR) [6]. The OCR continuously supervises grid current levels; when the measured current surpasses a predefined pickup threshold, it issues a trip command to the associated circuit breaker. A core objective of the current research is to assess how cyber-physical threats influence smart inverters, which may deliberately suppress or amplify fault currents to fall below detection thresholds, thereby preventing blinding failures [4, 6]. The study additionally considers daily fluctuations in PV irradiance under standard conditions and their effects on system voltage and current profiles. **Table 1** compiles a concise overview of contemporary research efforts aimed at bolstering smart grid robustness against cyber threats in DER-integrated environments [16–24]. Broadly, Piesciorovsky *et al.* [19], Aftab *et al.* [20], and Rajaei and Mazlumi [21] emphasized the effects of cyberattacks on power protection infrastructure.

In contrast, Peng *et al.* [5] and Liu and Li [15] focused on threats to microgrid control architectures. Zaki *et al.* [25] highlighted escalating protection challenges in active distribution networks arising from higher PV penetration and recommended a fault detection method tailored to PV-specific traits and associated uncertainties. Oliveira-De Jesus and Sorrentino [26] introduced an innovative technique for assessing distributed faults and OCR coordination in transmission corridors, incorporating time-dial and pickup adjustments.

Despite these contributions, relatively few works have examined protection schemes and PV control paradigms jointly. Accordingly, this research addresses the identified gaps in the existing body of knowledge outlined in **Table 1**. First, it applies a variety of cyber-attack scenarios to evaluate their influence on power protection devices and smart PV controllers. Second, the investigation utilizes a realistic network model to test different cyber intrusions. Third, the study analyzes transient behavior in an actual power system, including non-steady-state events triggered by switching actions, faults, or other disruptions. To facilitate this, the Electromagnetic Transients Program (EMTP) is employed, enabling detailed simulation of electrical system responses during transient episodes. Given the focus on power system stability assessment, EMTP was selected for its proficiency in modeling and evaluating critical stability aspects—including voltage stability, rotor angle stability, and small-signal stability—which serve as key metrics for dependable power network performance.

Table 1. Comprehensive overview of recent research efforts aimed at strengthening smart grid resilience against cyber threats in systems incorporating Distributed Energy Resources (DERs).

Ref.	Year	Protocol	Type of cyber attack	Study area	Standard or real network (DERs)	TYPE	Physical	Software	Cyber
Ahmed <i>et al.</i> [3]	2019	PMU	Data spoofing, Man-in-the-Middle (MITM)	√	×	IEEE-14	×	Real-Time Digital Simulator (RTDS)	√
Olowu <i>et al.</i> [4]	2020	×	False Data Injection (FDI)	×	√	IEEE-8500	PV	OpenDSS and MATLAB	×
Peng <i>et al.</i> [5]	2023	×	Stealthy Data Integrity Attacks (DIA)	×	√	IEEE-34	PV	Real-time Typhoon testbed	×
Yousefi kia <i>et al.</i> [6]	2023	×	FDI attacks and Denial of Service (DOS)	√	×	IEEE-14	×	MATLAB/Simulink	×
Zhou <i>et al.</i> [7]	2023	IEC61850	FDI	√	×	CIGRE	PV	Real-Time Digital Simulator (RTDS)	×
Liu and Li [15]	2023	PMUs	DOS	×	√	28 bus test system	PV	MATLAB	×
Kaewnukultorn <i>et al.</i> [16]	2023	×	DoS, intermittent attack, and modification attacks	×	√	×	PV	Power Hardware-in-the-Loop (P-HIL) test	×
Bamigbade <i>et al.</i> [17]	2023	PMUs	DoS and DIA	×	√	IEEE-14	PV	EMTP, MATLAB/Simulink	×
Zhang <i>et al.</i> [18]	2023	PMUs	DIA, replay attacks, and sophisticated attacks	×	√	IEEE-37	PV	OPAL-RT	×
Piescorovsky <i>et al.</i> [19]	2023	IEC61850	FDI and DOS	√	×	×	×	OPAL-RT	×
Aftab <i>et al.</i> [20]	2023	IEC 61850	FDI, DOS	√	√	IEEE-34 bus	PV	OPAL-RT	√

Rajaei and Mazlumi [21]	2023	×	FDI	√	×	IEEE-118 bus	×	MATLAB	×
Jadidi et al. [22]	2023	×	DIA	×	√	Microgrid benchmark	PV	×	×
Sowa and Monti [23]	2023	IEC61850	FDIA	√	√	×	PV	OPAL-RT	×
Elrawy et al. [24]	2023	GOOSE	FDIA	√	×	×	×	MATLAB/Simulink	×
Proposed study	–	IEC61850, GOOSE	FDI, DOS, MITM	√	√	Realistic power grid	PV	EMTP	√

Contributions

The primary outcomes and novel aspects of this investigation can be outlined as follows:

- Analyze and evaluate the effects of various cyber attacks—including False Data Injection (FDI), Denial of Service (DoS), and Man-in-the-Middle (MITM)—on smart PV control mechanisms and contemporary Overcurrent Relay (OCR) protection schemes operating under the IEC 61850 standard and GOOSE messaging protocol.
- Deliver a detailed understanding of the electrical and electromagnetic consequences arising from cyber intrusions when applied to realistic network parameters.
- Investigate how cyber attacks directed at the power grid influence the transient response characteristics of smart PV controllers and modern OCR-based protection systems.
- Develop a representative power network model in EMTP to examine transient phenomena and dynamic periods across multiple operating conditions: standard grid-connected mode, grid-connected mode experiencing sudden irradiation reductions, targeted cyber attacks on smart inverters, and combined physical faults with OCR involvement.

Problem Statement and Power Grid Methodology

The core focus of this work lies in designing and assessing an advanced adaptive protection scheme based on Overcurrent Relays (OCRs). Adaptive OCR configurations dynamically modify their parameters according to shifts between conventional grid topologies and those involving grid-tied PV integration. At the outset, breaker positions and grid status data are used to identify the current operational mode (grid-connected or islanded). A continuous supervision mechanism tracks changes in network topology relative to the prior configuration, retaining existing settings when no alterations occur. Appropriate setting groups for the primary Overcurrent Relay (OCRP) and backup Overcurrent Relays (OCRB)—prioritizing improved sensitivity and discrimination—are activated via communication channels, as depicted in Figure 1. Relay settings are chosen to minimize the overall tripping duration for OCRs during fault incidents. The tripping time for an OCR is calculated using Eq.1:

$$T = \frac{A}{\frac{I_{fault}}{I_{pick}} - 1} TMS \tag{1}$$

Where T represents the OCR operating time, A and B denote the constants defining the relay characteristic curve, I_{fault} is the measured fault current, I_{pick} is the pickup current setting, and TMS stands for the Time Multiplier Setting.

Figure 1 shows an example of a radial distribution system employing adaptive OCRs. In the event of a fault on one of the feeders, the primary relay (OCRP) is tasked with identifying the disturbance and isolating the affected section by opening its breaker. Should the OCRP fail to operate and clear the fault—potentially leaving healthy portions disconnected in certain fault conditions—the backup relay (OCRB) engages after an appropriate coordination delay. For illustration, consider a fault current (I_{fault}) of 2000 A: with the OCRP configured for $I_{\text{pick}} = 50$ A to accommodate load and cable thermal limits, utilizing the IEC normal inverse characteristic ($A = 0.14$, $B = 0.02$) and $TMS = 0.01$, the resulting tripping

time is $T = \left[\frac{0.14}{\left(\frac{2000}{50} \right)^{0.02} - 1} \right] \cdot 0.01 = 0.018$ s. The corresponding backup OCRB would then operate at 0.318 s, respecting

a coordination interval of 0.3 s.

However, a cyber attack capable of altering adaptive relay parameters, blocking trip commands, or disrupting communication links could lead to unnecessary disconnection of healthy feeders, widespread power quality issues, equipment damage, and loss of DER connectivity. Ultimately, such incidents would compromise the network's overall stability and the continuity of energy supply.

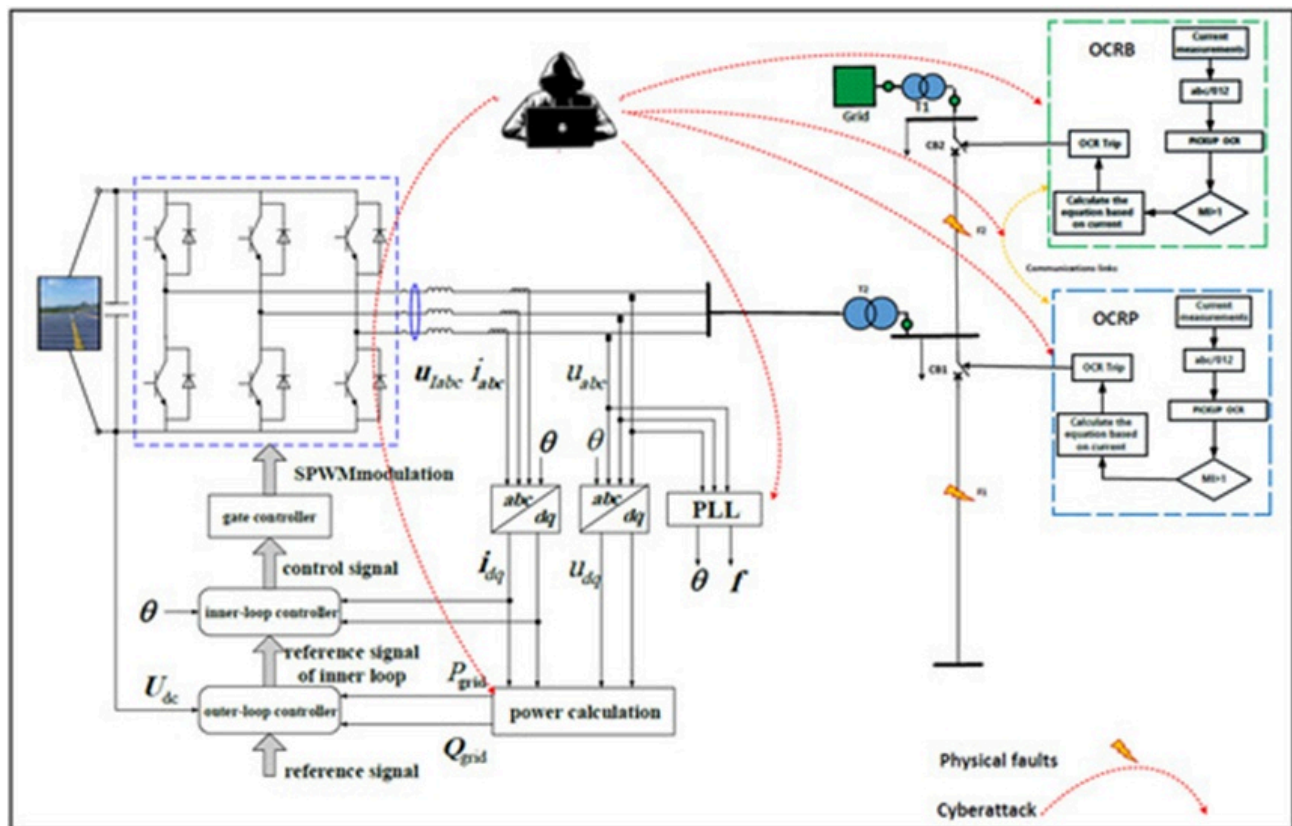


Figure 1. Configuration of the power system incorporating a grid-connected inverter and Overcurrent Relays (OCRs), subjected to both physical faults and cyber threats.

Furthermore, **Figure 1** depicts the layout of a grid-connected inverter system exposed to existing physical faults and various cyber threats. The modeling of smart-grid-following inverter control comprises several key elements, including the Phase-Locked Loop (PLL), filter, power controller, and current controller. These elements are typically implemented within the dq reference frame (direct-quadrature or synchronous reference frame). The primary function of the PLL is to detect

the actual system frequency (f) and generate a transformation angle that synchronizes the estimated frequency accordingly. In this study, the dynamic behavior of the smart grid-following inverter is illustrated in **Figure 1**, represented in a local dq-synchronous reference frame that incorporates the transformation angles (θ) defining the individual synchronous reference frames. Subsequently, the active and reactive power outputs (P_{grid} , Q_{grid}) are computed and supplied to the outer-loop controller. The outer-loop controller generates reference signals for the inner loop by comparing the measured P_{grid} , Q_{grid} , and capacitor voltage U_C with their respective reference values. As the power controller, this stage regulates the output power by setting the current reference commands for the inner-loop controller. The overall system dynamics depend critically on the inverter's behavior in combination with the current-limiting strategy implemented in the inner-loop controller. Ultimately, the control signals produced by the inner-loop controller are passed to the Sinusoidal Pulse-Width Modulation (SPWM) module to drive the smart inverter, as elaborated by Gonzalez et al. [27].

In a grid-connected inverter setup, Overcurrent Relays (OCRs) are effective at detecting faults due to significantly elevated current levels. The detailed examination presented here deepens understanding of the diverse cyber threats and fault conditions that can arise in smart grids powered by grid-connected inverters. The adoption of communication frameworks linking central control units with local controllers (inverters) has become a widely accepted practice in smart grid control architectures. The deployment of protocols such as IEC 61850 and Modbus constitutes a fundamental element of this approach [15, 27]. However, the presence of multiple vulnerabilities within the cyber layer introduces considerable risks. Attackers can exploit unsecured communication channels—characterized by the absence of built-in cybersecurity protocols, inadequate firewall protection, and insufficient overall security safeguards—posing a major threat.

Proposed Smart Power Network and Cyber Modeling

In actual power systems and smart grids, transient phenomena are non-steady-state events triggered by various events, including switching operations and faults. This study employs the Electromagnetic Transients Program (EMTP) to evaluate power network behavior under cyber-attack conditions. The EMTP facilitates a clear understanding of how electrical systems respond to short-duration disturbances, as illustrated in **Figure 1**. It is a well-established tool for deriving transient solutions in power systems and power electronics domains [28]. The simulation incorporates all relevant electrical conditions and formulates network behavior through differential equations. In EMTP, the impedance properties of capacitive and inductive components vary with frequency, necessitating detailed models of both electrical devices and control systems [28, 29]. By adopting time steps shorter than 50 microseconds, the EMTP model accurately captures the rapid dynamics induced by power electronic devices, such as voltage source converters, within the power system. In power networks and smart grids that integrate Distributed Energy Resources (DERs), converters typically serve as the interface between DER units and the distribution grid. EMTP simulations have become increasingly significant for studying the integration of renewable energy sources into contemporary power infrastructure. This includes tasks such as designing control strategies, assessing stability margins, and coordinating protection schemes. Moreover, the operational timescales of power protection relays and PV inverters fall within the domain of electromagnetic transient phenomena, as indicated in **Figure 2**. Consequently, it is essential to examine the effects of diverse cyber threats on realistic power systems and smart grids under transient conditions.

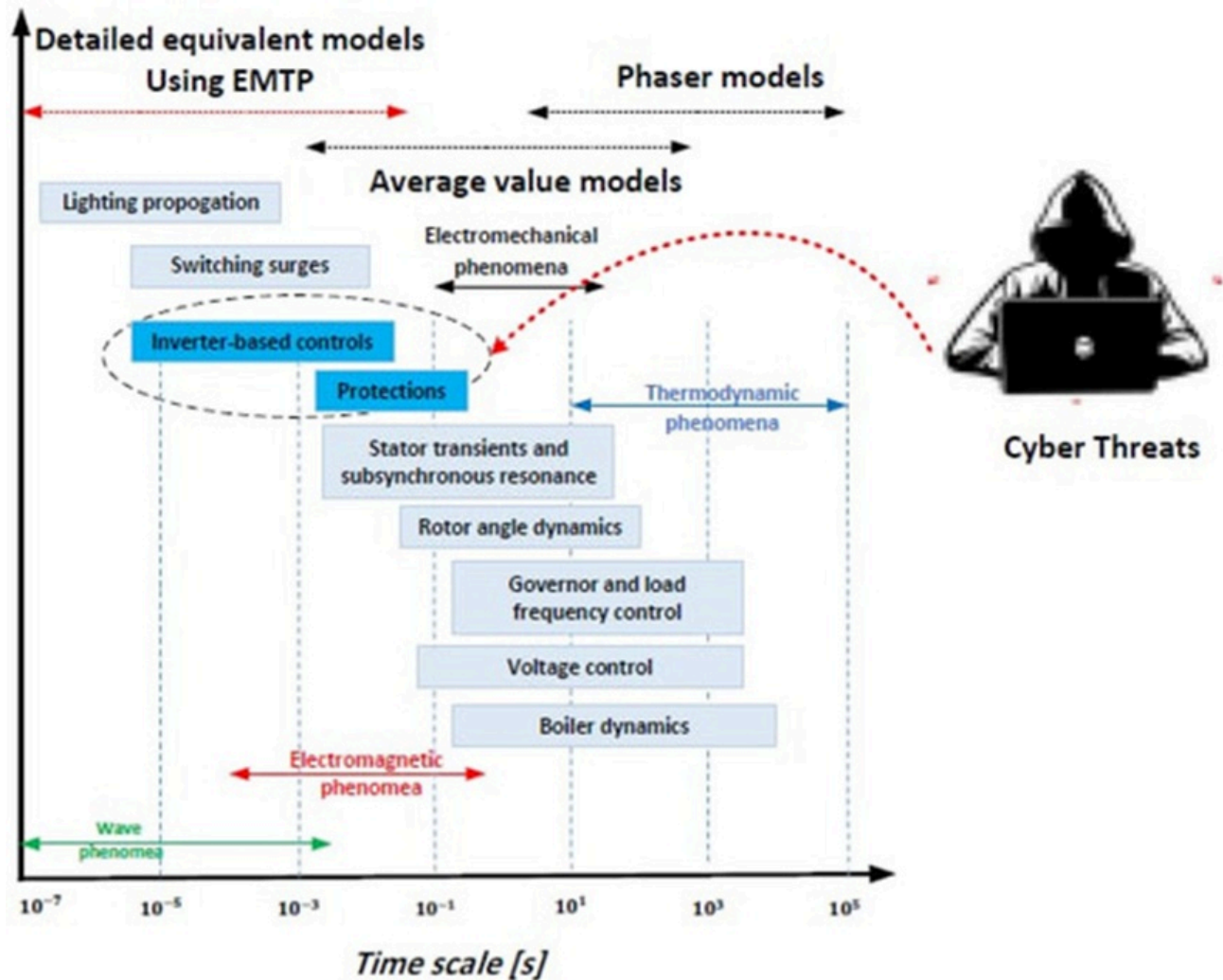


Figure 2. EMTP models are applied across various use cases.

The proposed smart power grid model

The electrical network modeled in this research replicates a realistic power distribution system. This grid is implemented and simulated within the Electromagnetic Transients Program (EMTP) environment, as depicted in [Figure 3](#). The configuration integrates conventional generation sources, represented by the utility feeder connected at Bus 10 (33 kV), with a 4 MWp photovoltaic (PV) farm. The PV farm connects to the 33 kV bus via four dedicated power transformers, labeled T15-T18. The farm is organized into four independent sections, designated P1 through P4, each with an installed capacity of 1 MWp, as shown in [Figure 3](#).

Additionally, multiple grid-connected PV systems (labeled G1 to G9) are interfaced on the low-voltage side of the network, playing a substantial role in meeting local energy demand, as further specified in [Table 2](#). As illustrated in [Figure 3](#), the entire power network is safeguarded by 12 Overcurrent Relays (OCRs). Two main step-down transformers (T13 and T14, 33/11 kV), visible in [Figure 3](#), supply the low-voltage (LV) portion of the system. Power is then further distributed via 12 distribution transformers (T1 to T12, 11/0.415 kV) to serve 37 individual buildings labeled B1 to B37. The extensive LV distribution network covers approximately 34,475 km², accommodates 37 buildings, and supports an annual electricity consumption of around 8.5 GWh, as detailed in [Table 3](#).

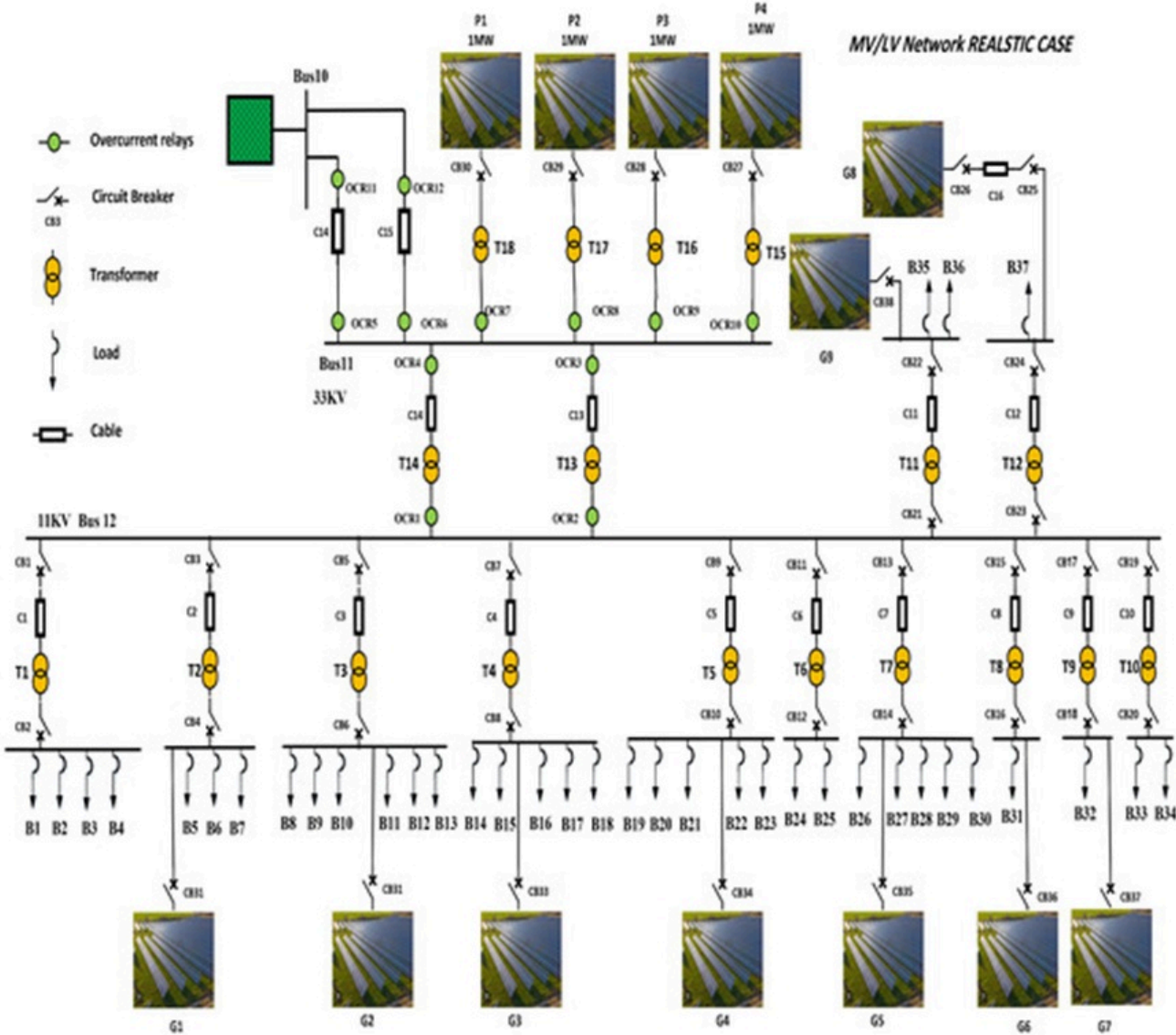


Figure 3. Schematic of the proposed smart power network.

Table 2. Specifications of the photovoltaic systems integrated into 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. Breakdown of load demand according to circuit breaker 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

Cyber-attack modeling

In intelligent grid environments, Intelligent Electronic Devices (IEDs) utilize the GOOSE protocol to facilitate the rapid exchange of essential protection and control messages. Time-critical operations—such as inter-tripping signals and blocking commands in protection schemes and inverter control—require delivery within 3 ms or less [18]. Consequently, GOOSE messages are mapped directly to the data link layer and employ the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) access method. By leveraging Ethernet switching capabilities, the GOOSE protocol supports

CSMA/CD operation in both multicast and full-duplex configurations, making it well-suited for real-time, mission-critical functions, including protection coordination and grid-tied PV system management. Upon detection of a state change, IEDs can simultaneously multicast GOOSE messages to multiple subscribers [19, 20]. To ensure reliable delivery, the GOOSE protocol employs two retransmission strategies: steady-state retransmission and fast retransmission. These strategies are governed by the Status (ST) number, which increments to signal a new event, and the Sequence (SQ) number, which increments for repeated transmissions of the same message content [21, 22].

In the present study, several targeted cyber attacks are applied to both control systems (smart PV inverters) and protection systems (OCRs), with analysis of their mutual cascading impacts and the effects on overall grid stability, as summarized in Table 4. The modeled attack types are grouped into three main categories:

Table 4. Overview of vulnerabilities and cyber-attack types considered for the proposed smart grid.

Vulnerability description	Relevance to cyber attacks
Weaknesses in the communication infrastructure	Reliance on protocols such as IEC 61850 that feature limited cybersecurity safeguards and inadequate protective measures. FDI: Exploitation through interception of unencrypted data streams. DoS: High exposure to denial-of-service disruptions.
Susceptibilities in smart inverter control logic	Proneness to unauthorized interference via cyber intrusions. FDI: Alteration of parameters and reference setpoints, resulting in deceptive control inputs for inner- and outer-loop regulation.
Limitations in adaptive overcurrent relay (OCR) configurations	Challenges arising from communication breakdowns or cyber vulnerabilities, where any delay or interruption in relay operation can compromise overall grid stability. MITM: Intentional delay of fault notification messages or obstruction of adaptive group setting updates. DoS: Suppression of trip commands, preventing relays from responding to detected faults.

Man-in-the-Middle (MITM): The adversary intercepts communication paths, allowing them to introduce delays or completely suppress selected messages. False Data Injection (FDI): This form of attack compromises data integrity by inserting falsified information, thereby manipulating setpoints and protection parameters. Denial-of-Service (DoS) Attack: The attacker disrupts connectivity to one or more grid elements, preventing them from responding appropriately to detected faults and thereby jeopardizing system stability.

Cyber threats targeting the power protection system (OCR)

Intelligent Overcurrent Relays (OCRs) play a critical role in the protection framework of electrical grids. Their primary responsibility is to identify fault conditions and promptly isolate the impacted portions of the network. To ensure proper coordination, these relays typically incorporate a backup relay (OCRB) located upstream from the primary relay (OCRP), as illustrated in Figure 3. In Distribution Networks (DNs) characterized by numerous Distributed Energy Resource (DER) integration points, protection coordination grows significantly more challenging [2, 3]. Consequently, adaptive OCR configurations are essential for handling dynamic variations in network topology, generation output, and load demand by switching among different relay setting groups [6]. Conventional fixed protection schemes often prove inadequate in responding to such variability [6, 7]. Deploying adaptive protection introduces considerable challenges, particularly concerning communication disruptions, storage of setting parameters, implementation of operating characteristic curves, and exposure to cyber vulnerabilities. Any interference that prevents or postpones relay operation can therefore jeopardize grid stability. In the present study, three principal cyber-attack strategies are applied to the protection system depicted in Figure 2:

- **Manipulation of Group Settings:** The adversary prevents adaptive OCRs from updating to the appropriate group setting or intentionally delays the transition for a specified duration (via False Data Injection–FDI).
- **Delaying Fault Messaging:** Through a Man-in-the-Middle (MITM) attack, the attacker introduces latency in the transmission of fault detection information. This delay impairs the grid's timely response capability, potentially leading to instability.

Cyber threats targeting smart PV inverters

The in-depth evaluation conducted in this research deepens insight into possible cyber vulnerabilities and fault conditions affecting smart grids that rely on grid-connected inverters. Integrating communication links between centralized control units and local inverter controllers has become standard practice in smart grid management, often using protocols such as IEC 61850 and Modbus, as shown in **Figure 1** and **Table 4** [15, 27]. Vulnerabilities present in the cyber domain pose serious risks, since unprotected communication channels—lacking built-in security features, robust firewalls, or adequate protective measures—remain open to exploitation by malicious actors. Such weaknesses are particularly susceptible to various cyber intrusion techniques, including False Data Injection Attacks (FDIAs). Under normal operating conditions, IEEE 1547-2018 requires that inverters' reactive power output remain stable [5, 15]. However, when an attack compromises the inverters and alters the reactive power reference value, excessive current may be drawn from the grid. This abnormal behavior can trigger OCR devices to detect a fault and disconnect from the main grid. The described manipulation can effectively circumvent active protective functions by falsifying control references for both inner- and outer-loop controllers, thereby deceiving the core inverter regulation logic. To replicate realistic cyber threats, four distinct attack signal types—based on the classifications provided in Liu and Li [15]—are modeled as follows:

- **Continuous Pulse Signal:** The attacker injects recurring malicious perturbations, transforming the legitimate data stream into a periodic square-wave pattern.
- **Scaling Signal:** The attack applies a multiplicative scaling factor to distort the original signal magnitude.
- **Sine Signal:** The authentic data are overlaid or replaced with a sinusoidal waveform characterized by a specific amplitude factor.
- **Ramp Signal:** The manipulated control signal assumes the form of a linearly increasing (ramp) waveform.

Results and Discussion

The smart grid configuration, encompassing adaptive Overcurrent Relays (OCRs) and grid-connected smart inverters, has been implemented for the medium-voltage/low-voltage (MV/LV) network model shown in **Figure 2**. This MV/LV representation is constructed using real-world network parameters and measurements, with its behavior evaluated under a range of cyber-attack conditions. The purpose of this section is to present and interpret the transient simulation outcomes derived from multiple physical fault scenarios. The analysis begins by examining the proposed network's performance in the absence of cyber attacks, including a case involving a sudden reduction in irradiation. Next, the effects of various cyber intrusions on the protection system (OCR) and smart inverter operation are demonstrated. Additionally, transient profiles of key electrical quantities—voltage, current, active power, and reactive power—are illustrated for the proposed network. In summary, this section evaluates the consequences of simulated cyberattacks on overall grid behavior during a 1-second transient window. To provide a reference, baseline performance is first established by recording normal grid operation in the absence of faults or malicious interventions. The primary monitored variables throughout the assessment include:

- Voltage at the PV bus (or Point of Common Coupling – PCC bus).
- DC-link voltage of the PV system (measured at the inverter).

- AC output of the PV system (measured at the inverter).
- Solar irradiation level.
- Direct-axis and quadrature-axis currents (I_d and I_q) at the grid interface.
- Active and reactive power exchanged with the grid.

The proposed power network under normal operating conditions

To establish a performance benchmark for the proposed power grid and to enable meaningful comparisons across diverse cyber-attack scenarios, the system was first analyzed under standard steady-state conditions (in the absence of any cyber intrusions or physical faults).

In this phase of the study, the behavior of the photovoltaic (PV) system is assessed during normal operation, assuming constant load demand and irradiation levels, with no faults or malicious interventions present. The solar irradiation is held steady at 1000 W/m^2 , and the simulation spans 1 s to capture relevant transient phenomena within the scope of this investigation, as depicted in **Figure 4**. The initial period (up to approximately 0.04 s) reflects the transient response associated with synchronizing and connecting the PV system to the grid. In the subsequent steady-state phase, the results demonstrate a stable grid configuration, with the voltage at the Point of Common Coupling (PCC) bus maintained at 33 kV. The PV system delivers an AC of 25 A, corresponding to an active power output of 1 MW. Note that the evaluation here pertains to a single PV unit. Furthermore, the direct-axis current component (I_d) stabilizes at a constant 1.25 A, while both the reactive power and the quadrature-axis current (I_q) remain at zero. This detailed assessment highlights the reliability and equilibrium of the PV system under ideal operating conditions, offering valuable reference data for its baseline performance characteristics.

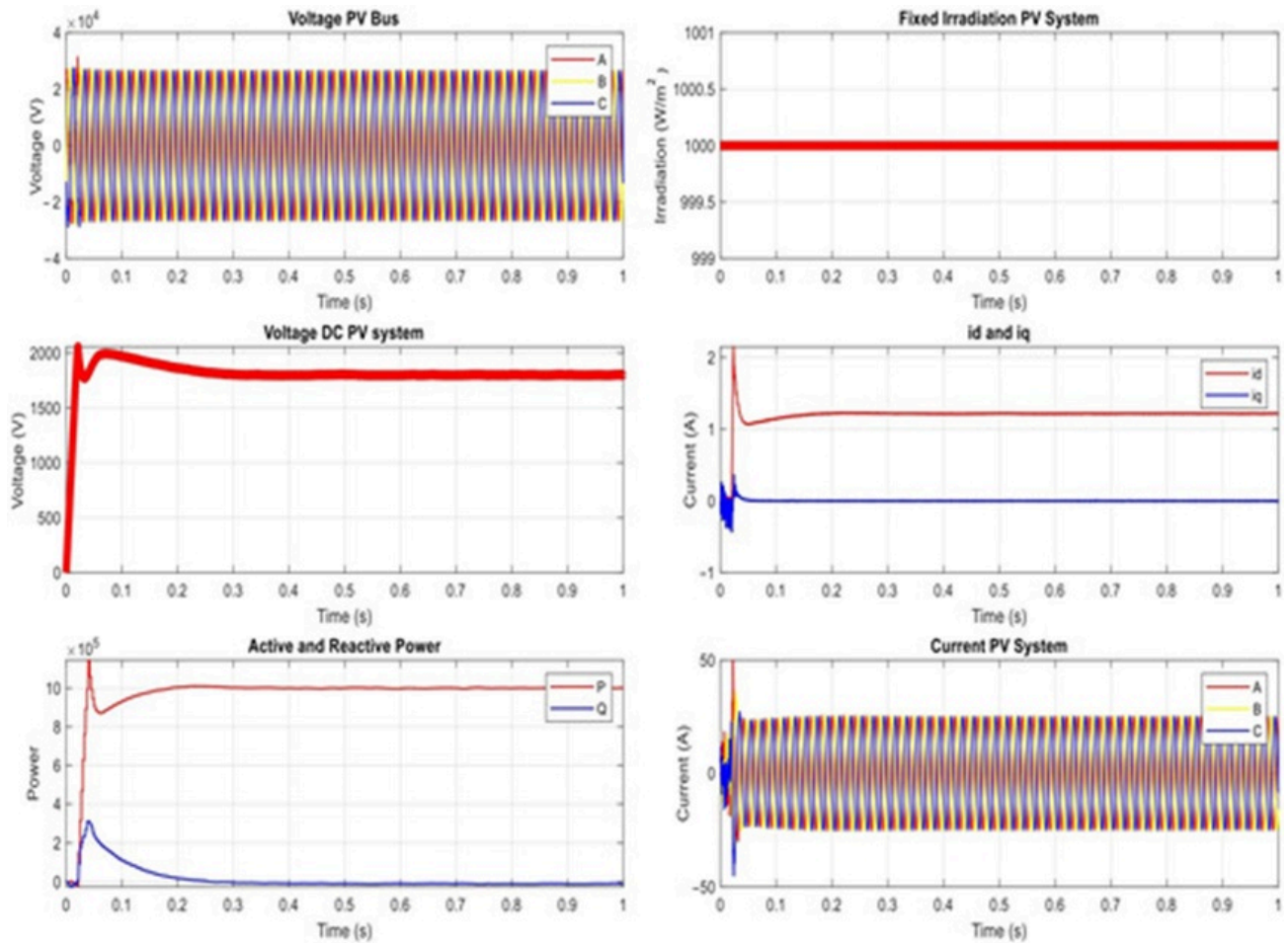


Figure 4. Performance metrics of the proposed power network during normal operation with constant irradiation levels.

To further validate the proposed network model, the study investigates the PV system's response to temporary reductions in solar irradiation under otherwise normal operating conditions. Specifically, at $t = 0.4$ s, the irradiation level drops from 1000 W/m^2 to 800 W/m^2 for a duration of 0.1 s, then rises to 900 W/m^2 and remains there for 0.2 s before returning to the nominal 1000 W/m^2 for the remainder of the simulation, as illustrated in **Figure 5**. During the initial reduction (0.4 – 0.5 s at 800 W/m^2), the DC-link voltage falls to 1500 V , the PV system current decreases to 17 A , and the active power output reduces to 0.7 MW . Reactive power remains at zero throughout, although noticeable variations in active power occur. When irradiation increases to 900 W/m^2 , active power recovers to 0.9 MW before returning to the original 1 MW once irradiation resumes at 1000 W/m^2 . These power fluctuations directly influence the current magnitudes, while the PCC voltage remains essentially constant. This analysis provides important insights into the transient and dynamic responses of photovoltaic systems to variations in solar irradiance and their effects on power delivery and current profiles.

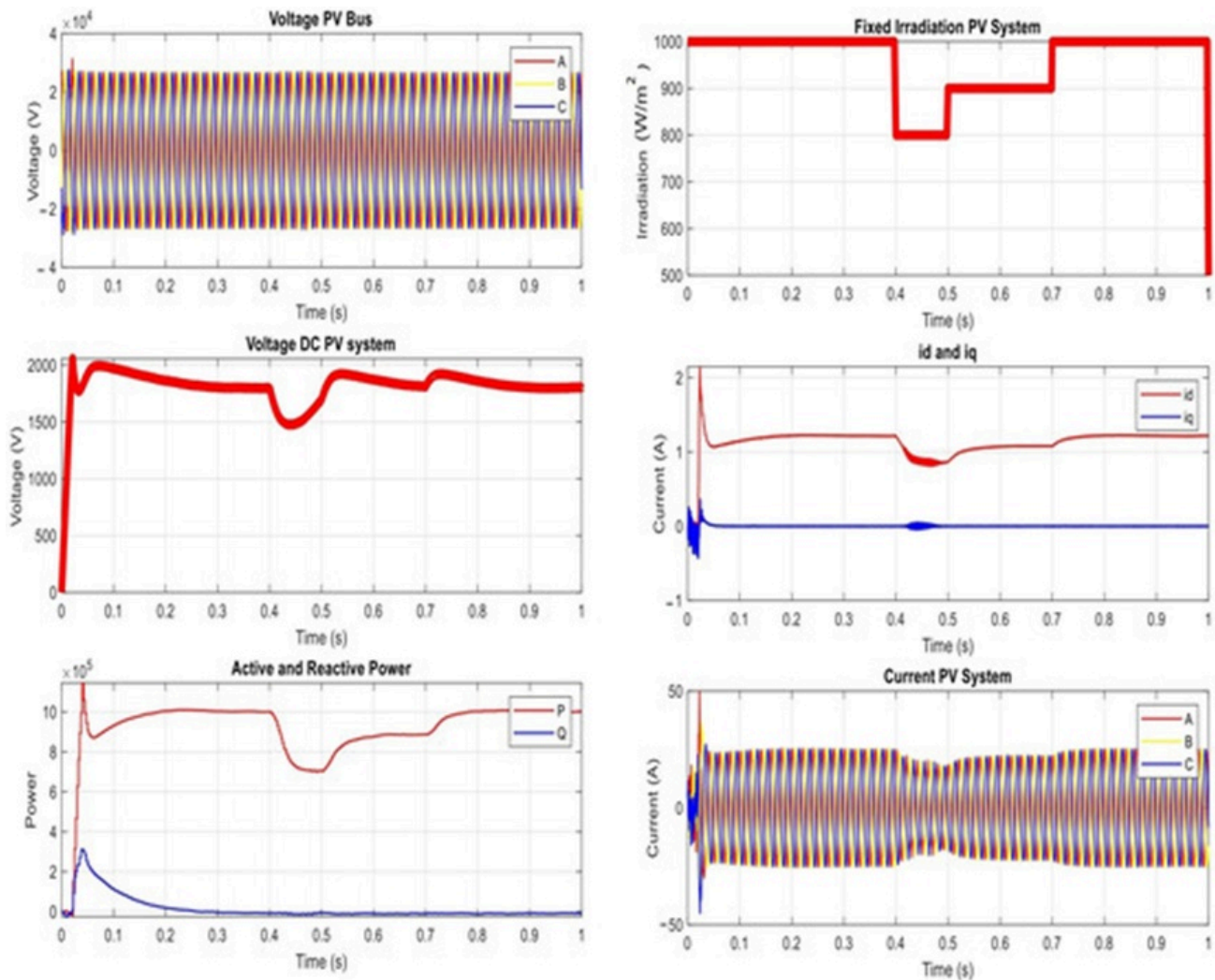


Figure 5. Performance metrics of the proposed power network during normal operation under varying irradiation levels.

Results of of cyber threats on power protection system (OCR)

The deployment of adaptive Overcurrent Relay (OCR) schemes, while advantageous, introduces vulnerabilities—particularly related to communication disruptions and cyber threats. Any interference that blocks or delays relay action can therefore seriously compromise grid stability. This subsection examines three key cyber-attack strategies directed at the protection system shown in [Figure 2](#).

Manipulating group settings

In this attack scenario, the adversary employs False Data Injection (FDI) to prevent adaptive OCRs from switching to the correct group settings or to delay the transition. A physical three-phase fault is introduced on the low-voltage side of transformer T14 at $t = 0.5$ s, as presented in [Figure 6](#). At $t = 0.67$ s, the attacker modifies the group settings of the primary relay (OCR4) and backup relays (OCR11 and OCR12) by prematurely activating the backup group settings intended for islanded operation mode. This misconfiguration causes a pronounced voltage drop and high ripple at the PCC bus, accompanied by a sharp increase in PV system current, as visible in [Figure 6](#). The grid's reliance on PV generation leads to a rapid rise in DC-link voltage, accompanied by significant ripple. Similar oscillatory behavior is observed in the I_d , I_q , active power, and reactive power waveforms. These severe deviations ultimately trigger disconnection actions by other protection devices, resulting in complete system isolation.

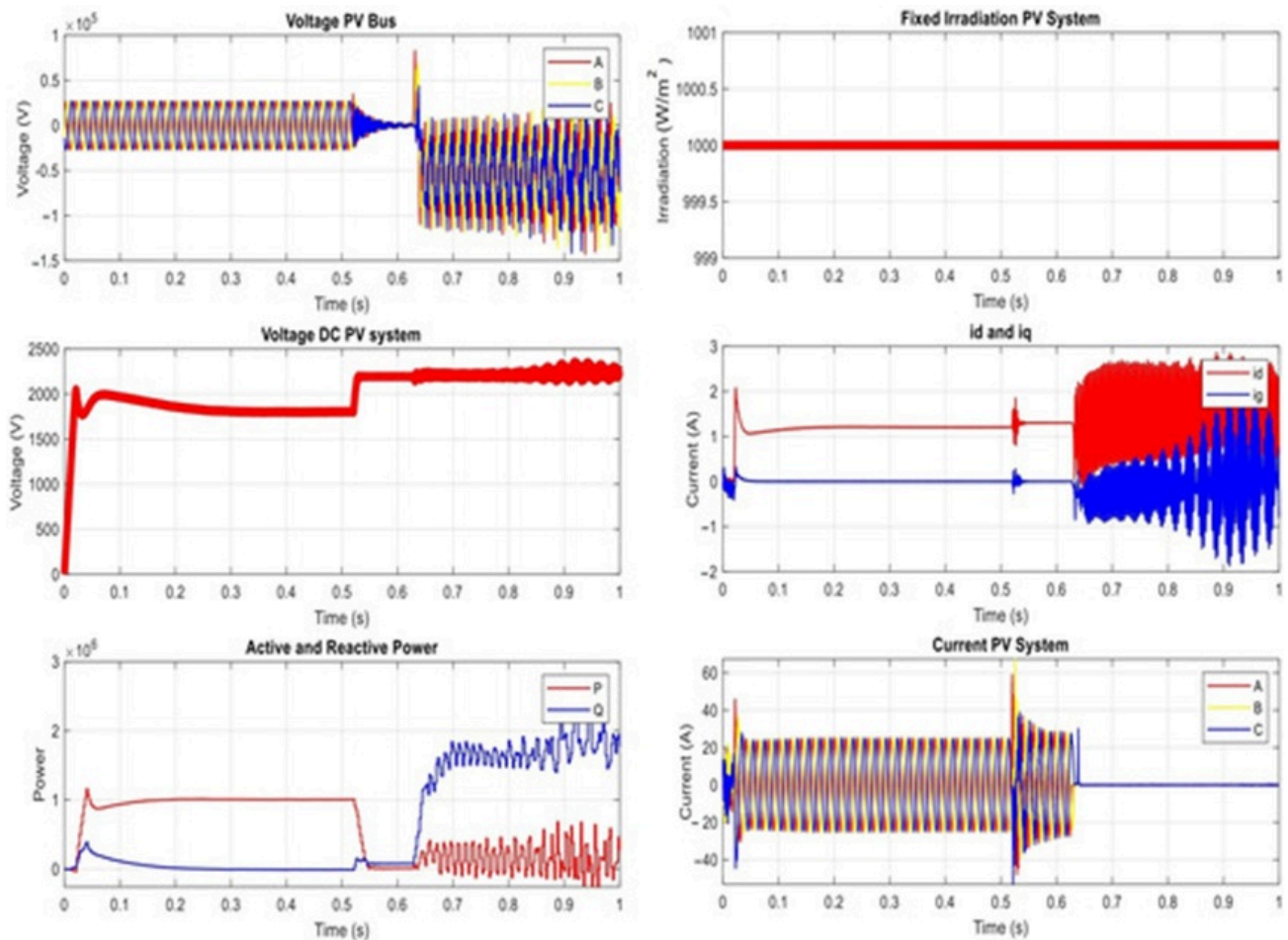


Figure 6. Performance of the proposed power network under a manipulating-group-settings attack targeting the OCRs.

Delaying fault messaging

Here, the attacker uses a Man-in-the-Middle (MITM) technique to introduce intentional delays in the communication path between the adaptive OCRs and the circuit breaker following fault detection. Such interference prevents timely fault clearance, potentially destabilizing the grid, as demonstrated in **Figure 7**. In this case, a physical three-phase fault occurs on the low-voltage side of transformer T14 at $t = 0.5$ s. The attacker delays transmission of the tripping command from the adaptive OCRs to the breaker by approximately 0.3 s. This prolonged fault duration produces substantial ripple in active and reactive power as well as in PV system current before eventual clearance, as shown in **Figure 7**. Consequently, secondary protection mechanisms activate, disconnecting the PV system and forcing the grid to operate solely on the utility supply.

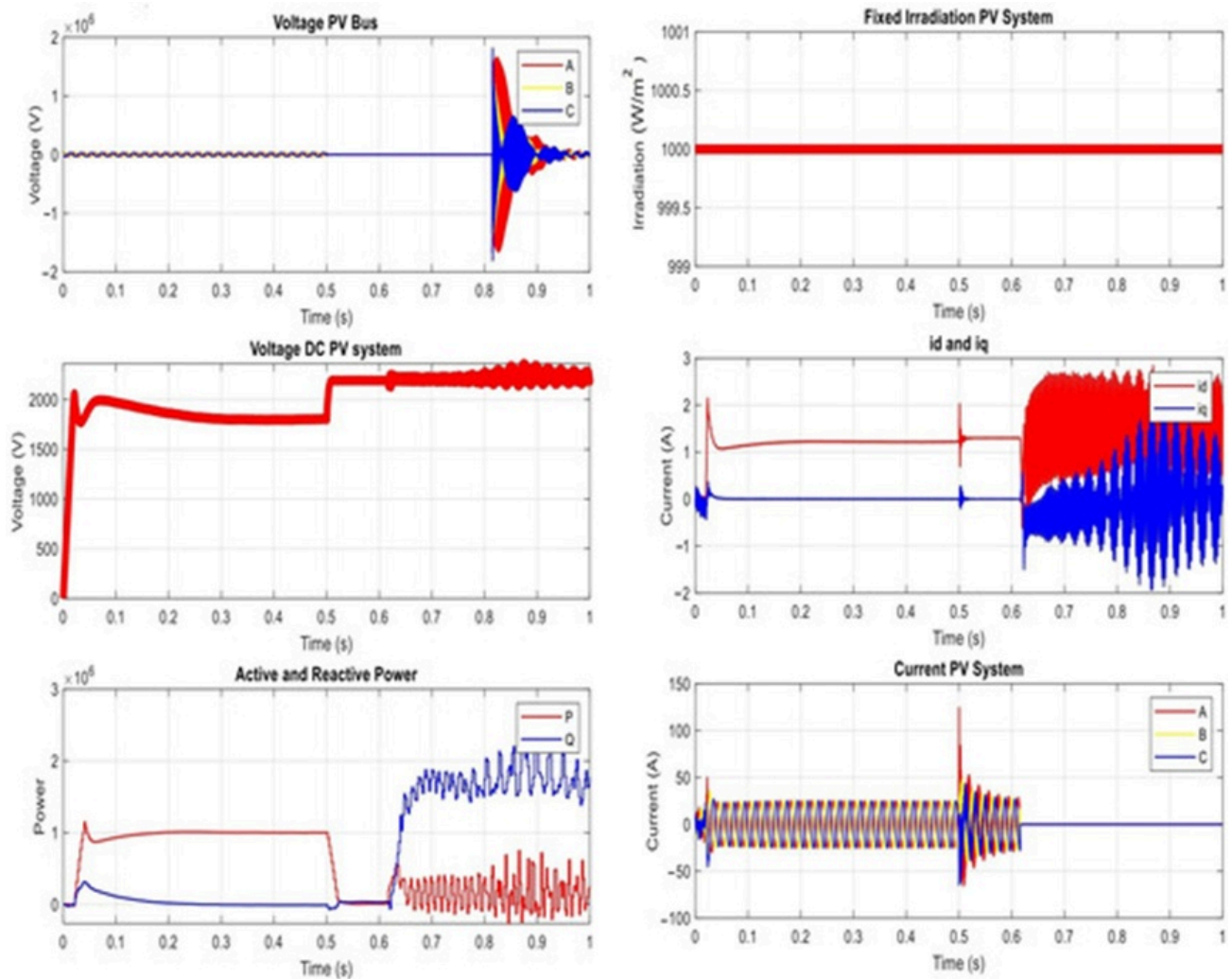


Figure 7. Performance of the proposed power network under a delaying-fault-messaging attack on the transformer side.

In another scenario, the adversary intercepts and suppresses fault-indication messages generated by the Overcurrent Relay (OCR) at the PV farm (OCR10), as depicted in Figure 2. By intentionally delaying the delivery of essential fault data to the circuit breaker, the attacker aims to establish a protection blind spot through a combined Man-in-the-Middle (MITM) and message-dropping strategy. In this case, a physical three-phase fault is introduced on the PV farm side of transformer T15 at $t = 0.5$ s. The attacker delays the tripping command from the adaptive OCRs to the circuit breaker by approximately 0.3 s. During this extended delay, the fault current surges to 5000 A.

As a consequence, the total active power output from all PV systems collapses to zero, as illustrated in Figure 8. The grid's heavy reliance on PV generation leads to rapid DC-link voltage escalation, accompanied by pronounced ripple. Comparable oscillatory patterns are evident in the direct-axis current (i_d) and quadrature-axis current (i_q) throughout the delay interval.

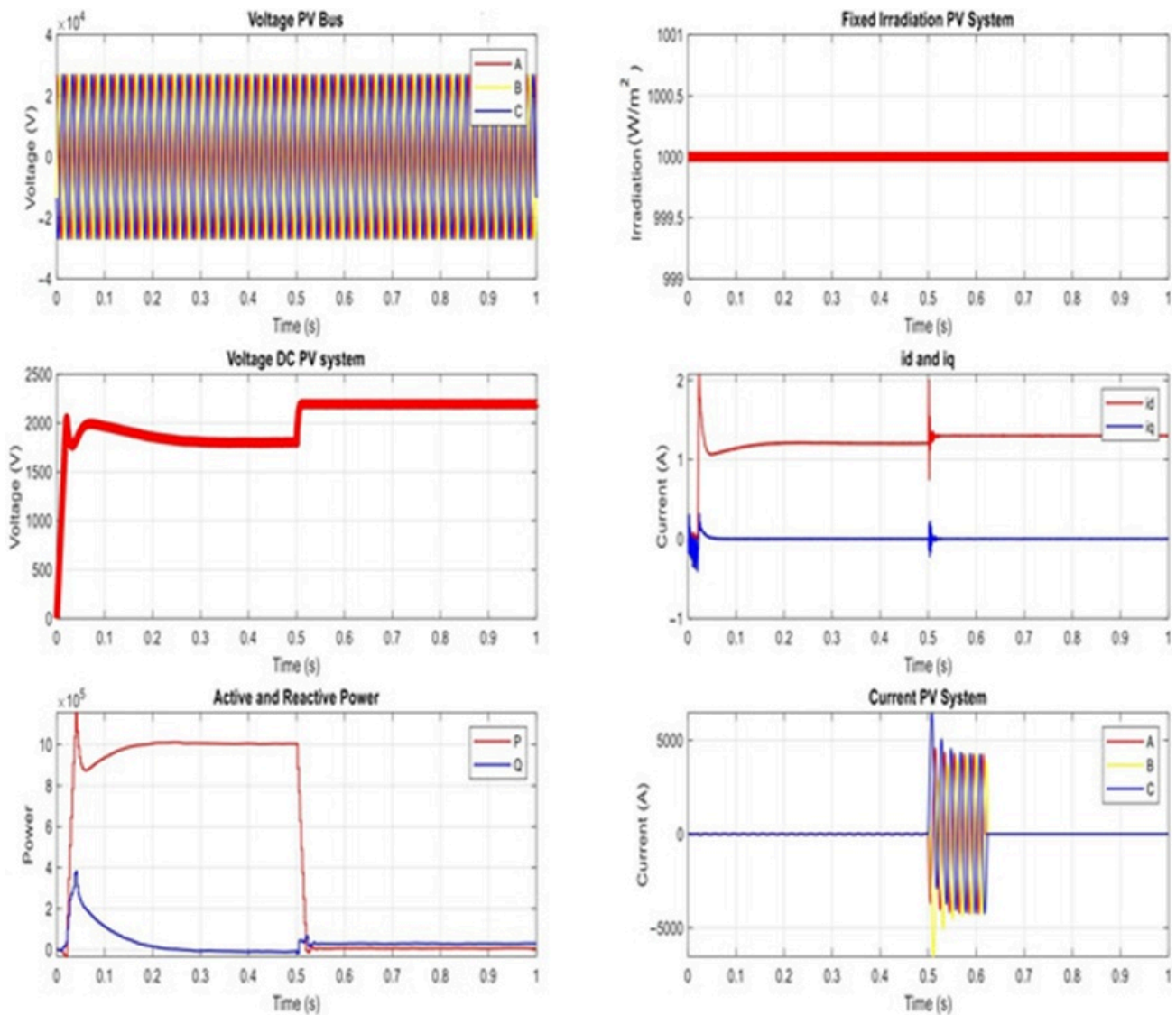


Figure 8. Performance of the proposed power network under a delaying-fault-messaging attack applied on the PV farm side.

Results of cyber threats on the smart PV inverters

As shown in **Figure 3**, the active power (P_{grid}) and reactive power (Q_{grid}) are computed and supplied to the controller. Functioning as the power controller, this module regulates the PV system's output by directing the smart inverter to produce the desired active power (P) and reactive power (Q). Under normal operating conditions, the reactive power contribution from the PV inverter remains zero, as demonstrated in **Figures 4 and 5**. In situations involving voltage sags, the inverter injects a controlled amount of reactive power to support voltage stability. The present study evaluates four primary attack strategies targeting the smart inverter control loop, each designed to force unwanted reactive power injection into the grid under otherwise normal conditions. In this part of the investigation, the behavior of the PV system and the connected power grid is assessed under standard operating conditions while subjected to targeted control attacks on the inverter as detailed below:

Continuous pulse signal attack

The attacker targets the PV inverter's reactive power regulation capability. In this case, the command signal for reactive power injection is assumed to be a pulsed waveform, as shown in **Figure 9**. The pulses are extremely brief, with 10

occurring within a 0.1 s interval. Initially, this causes an elevation in current at the source bus; however, the OCR fails to identify the anomalous condition and does not initiate disconnection. As shown in **Figure 10**, at $t = 0.5$ s, the reactive power injected into the system reaches 2 MW. The PV system current exhibits severe ripple and harmonic distortion, with peak amplitudes approaching 50 A. The DC-link voltage waveform also displays marked distortion attributable to the attack. Since the perturbing signal is intermittent rather than sustained, the protection system does not register the irregularity and therefore takes no corrective action. This lack of response to abnormal power flow results in substantially elevated harmonic content in the PV system current and correspondingly higher losses.

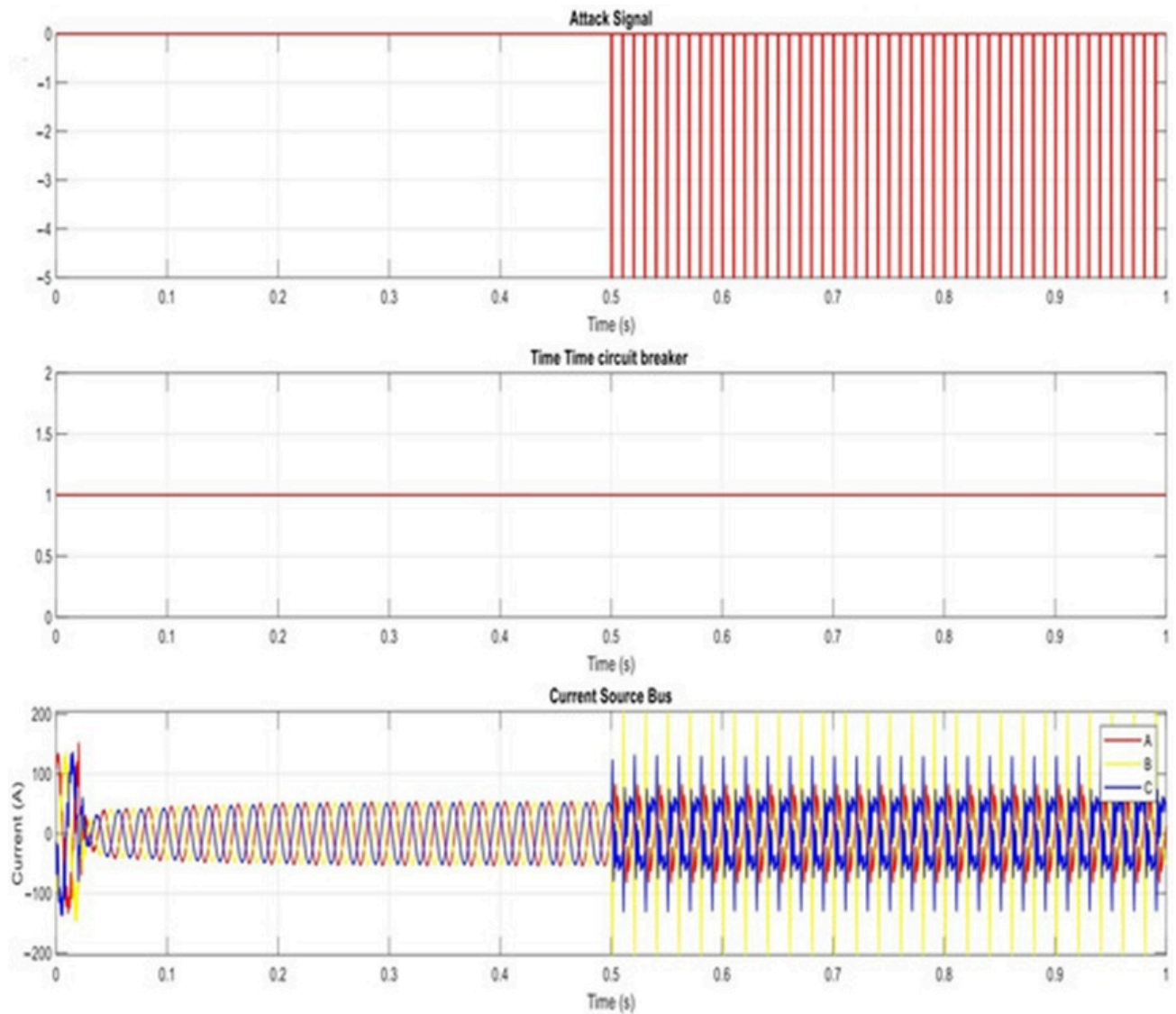


Figure 9. Continuous pulse signal attack applied to the PV inverters.

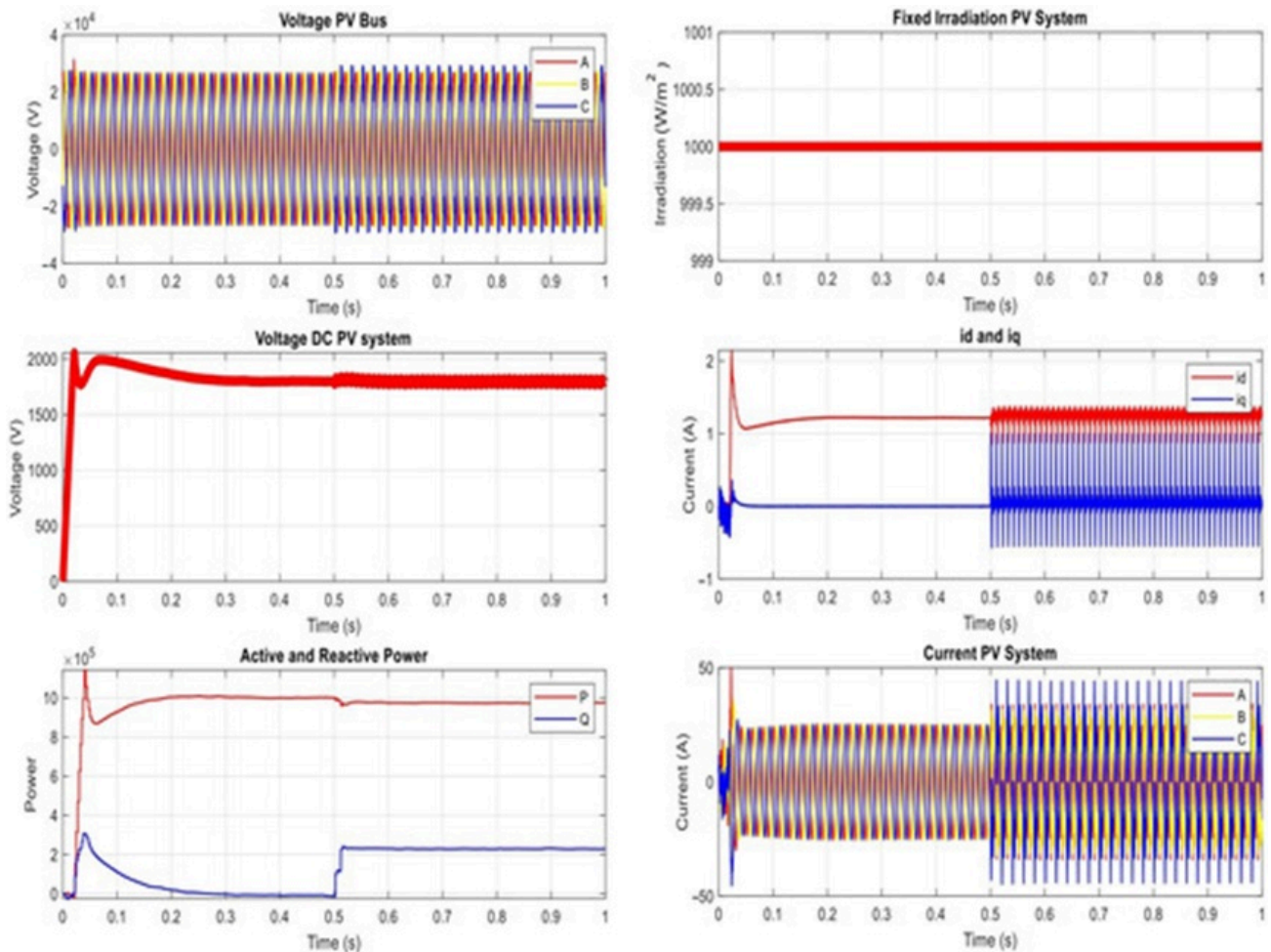


Figure 10. Performance of the proposed power network under a continuous pulse signal attack on the PV inverters.

Scaling signal attack

The attacker manipulates the PV inverter's reactive power control function. In this instance, the reactive power injection command follows a scaled waveform pattern, as illustrated in **Figure 11**. Compared with the pulse attack, the disturbance duration is notably longer, with a single extended pulse lasting 0.1 s. This leads to a subsequent increase in current at the source bus. In contrast to the previous case, the OCR successfully detects the abnormality and trips the fault at the PV farm side at $t = 0.65$ s, as indicated in **Figure 11**. During the early phase of the attack (0.5–0.6 s), the PV system current rises while the overall system remains stable. However, in the later phase, when the reactive power command is scaled down to -7 , pronounced current disturbances are observed, as shown in **Figures 11 and 12**. The PV system's DC-link voltage exhibits significant reductions and oscillations, dropping to as low as 1400 V, as shown in **Figure 12**. These voltage drops coincide with a sharp current surge at the source bus. Ultimately, the protection system isolates the utility connection, forcing the grid to rely solely on PV generation and resulting in system instability.

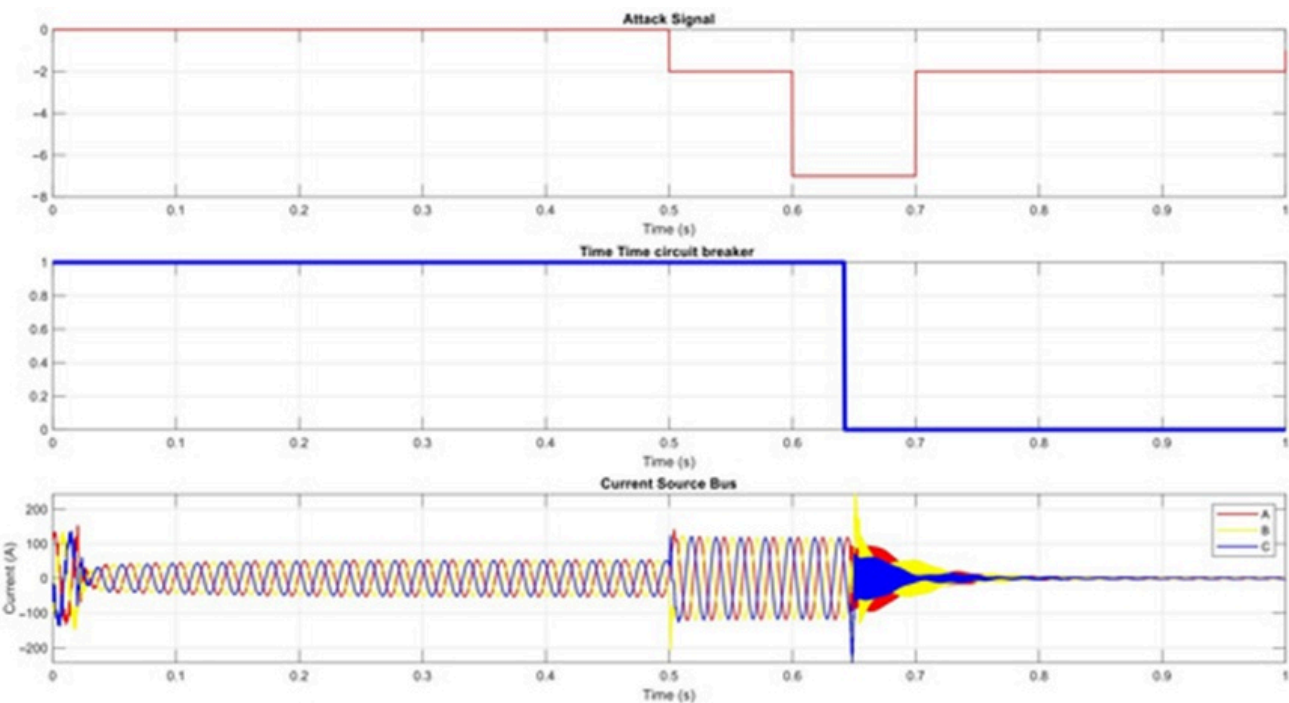


Figure 11. A scaling signal attack is applied to the PV inverters.

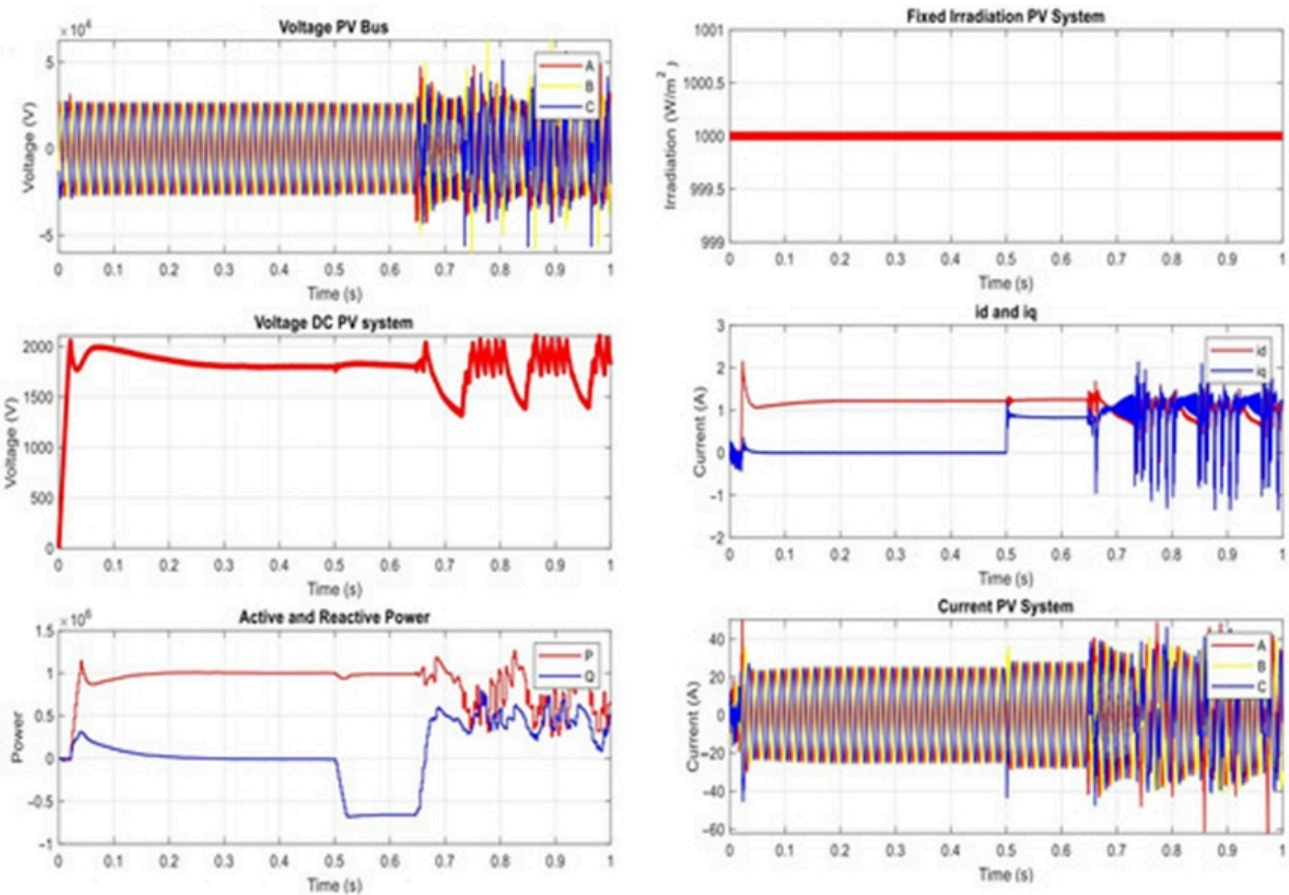


Figure 12. Performance of the proposed power network under a scaling signal attack on the PV inverters.

Sine signal attack

The attacker compromises the PV inverter's control mechanism by modulating the reactive power injection command. In this instance, the regulating signal has a sinusoidal waveform oscillating between ± 5 , as depicted in **Figure 13**. The disturbance lasts longer than the continuous pulse attack but remains shorter than the scaling attack. Consequently, the Overcurrent Relay (OCR) requires additional time to identify the anomaly and initiate disconnection at $t = 0.7$ s, later than the 0.65 s response observed in the scaling attack scenario. During the early stage of the intrusion (0.5–0.7 s), the PV system current exhibits a clear rise, accompanied by a pronounced ripple in the DC-link voltage, active power (P), and reactive power (Q), as illustrated in **Figure 14**. As a result, the protection scheme isolates the PV system from the utility grid, shifting the entire load dependency onto the utility supply. At $t = 0.7$ s, the utility connection is severed. Following this isolation, the PV system's active power output declines sharply from its nominal 1 MW to approximately 0.5 MW. The overall PV installation becomes destabilized due to the sustained effects of the attack.

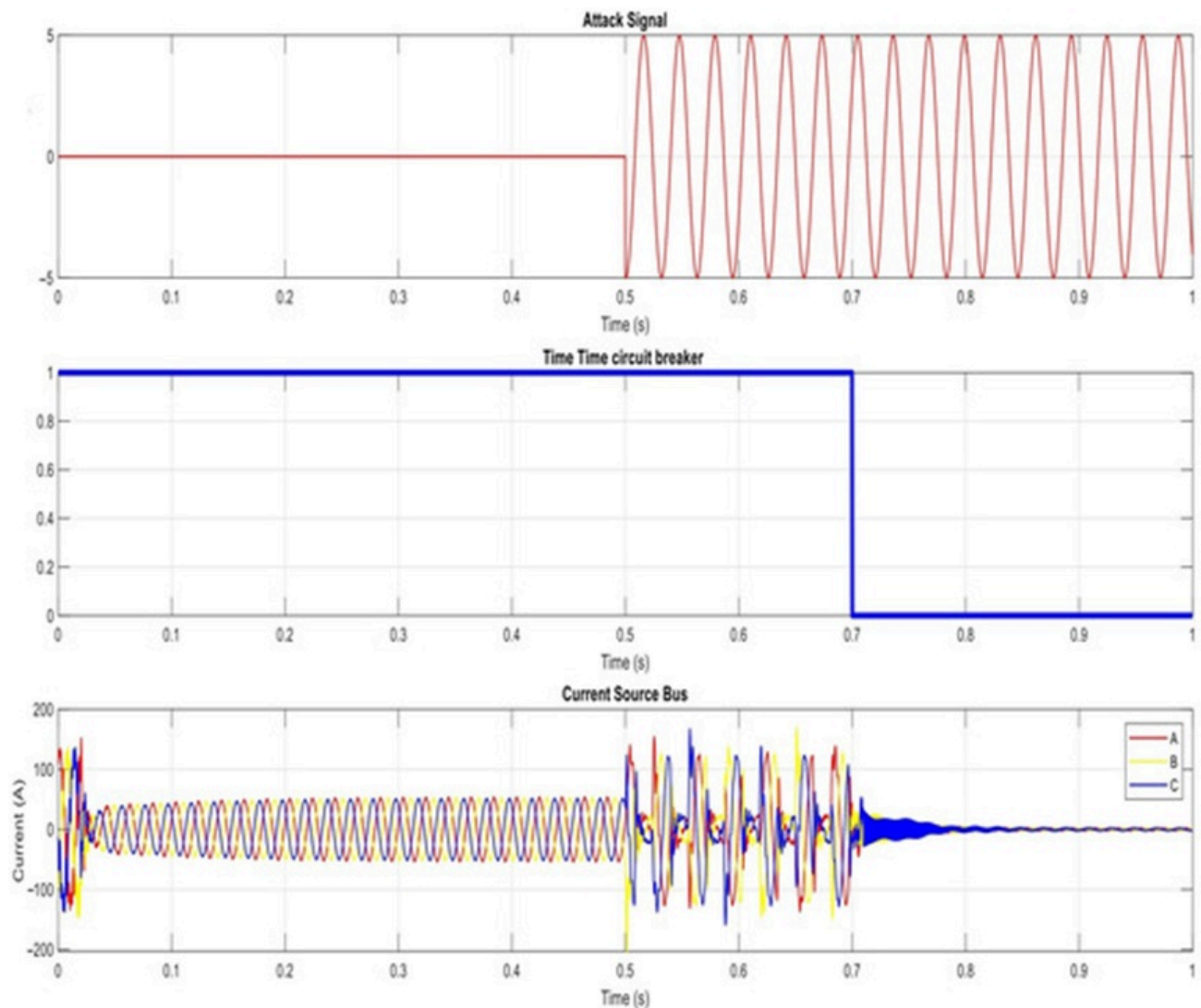


Figure 13. Sine signal attack applied to the PV inverters.

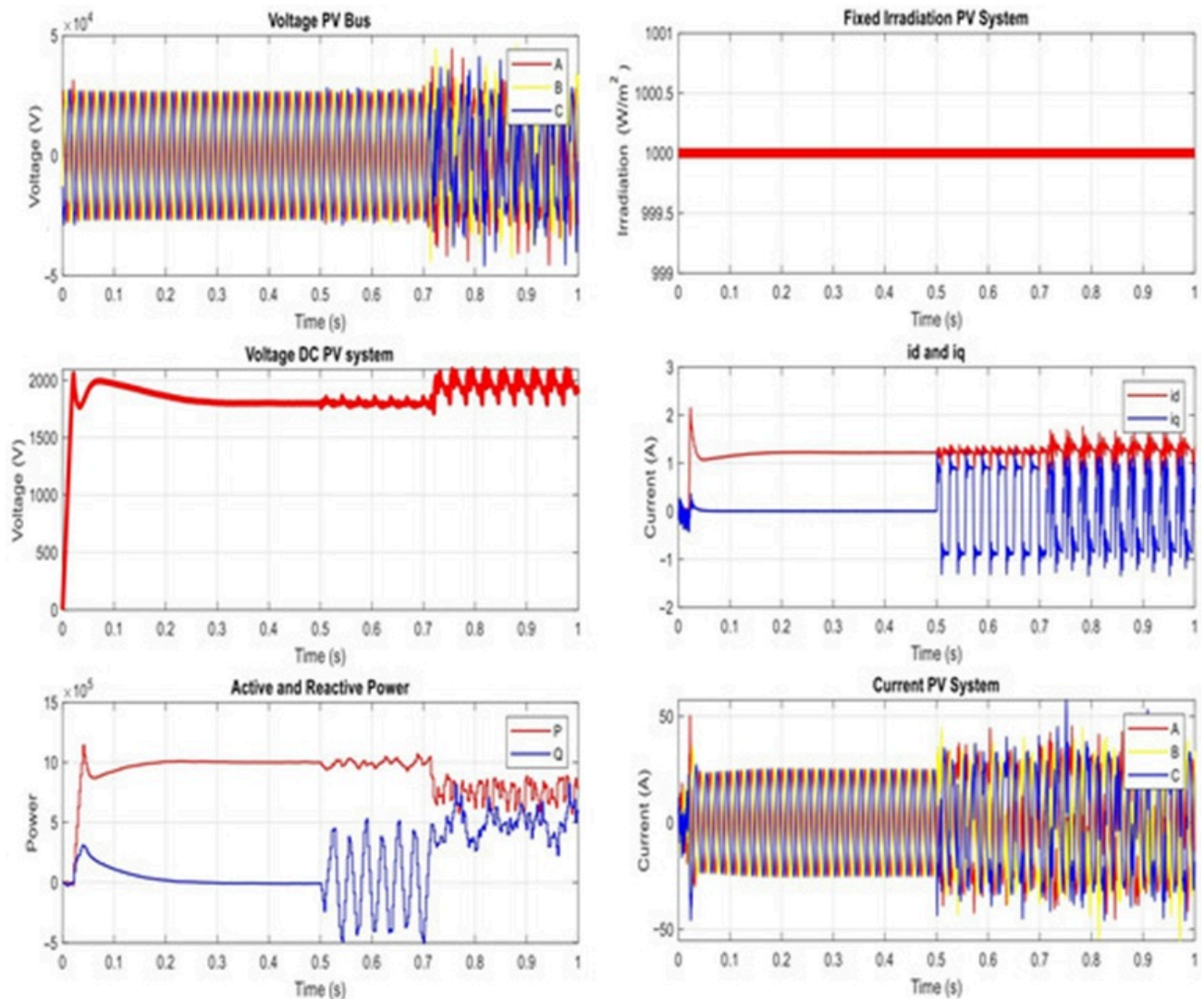


Figure 14. Performance of the proposed power network under a sine-wave attack on PV inverters.

Ramp signal attack

The ramp signal attack involves a control command for reactive power injection that follows a linearly decreasing ramp waveform. As shown in **Figure 15**, the signal progressively falls from 0 to -5 . Owing to the steady and continuous nature of the disturbance, the OCRs detect the irregularity more rapidly and isolate the PV system at $t = 0.65$ s—faster than the 0.7 s disconnection time required in the sine signal case. In the initial phase (0.5 – 0.65 s), the PV system current increases noticeably while significant oscillations appear in the DC voltage, active power (P), and reactive power (Q), as visible in **Figure 16**. Subsequently, the protection system swiftly disconnects the photovoltaic (PV) link from the utility, leaving the network operating solely on utility power and rendering it fully dependent on the main grid.

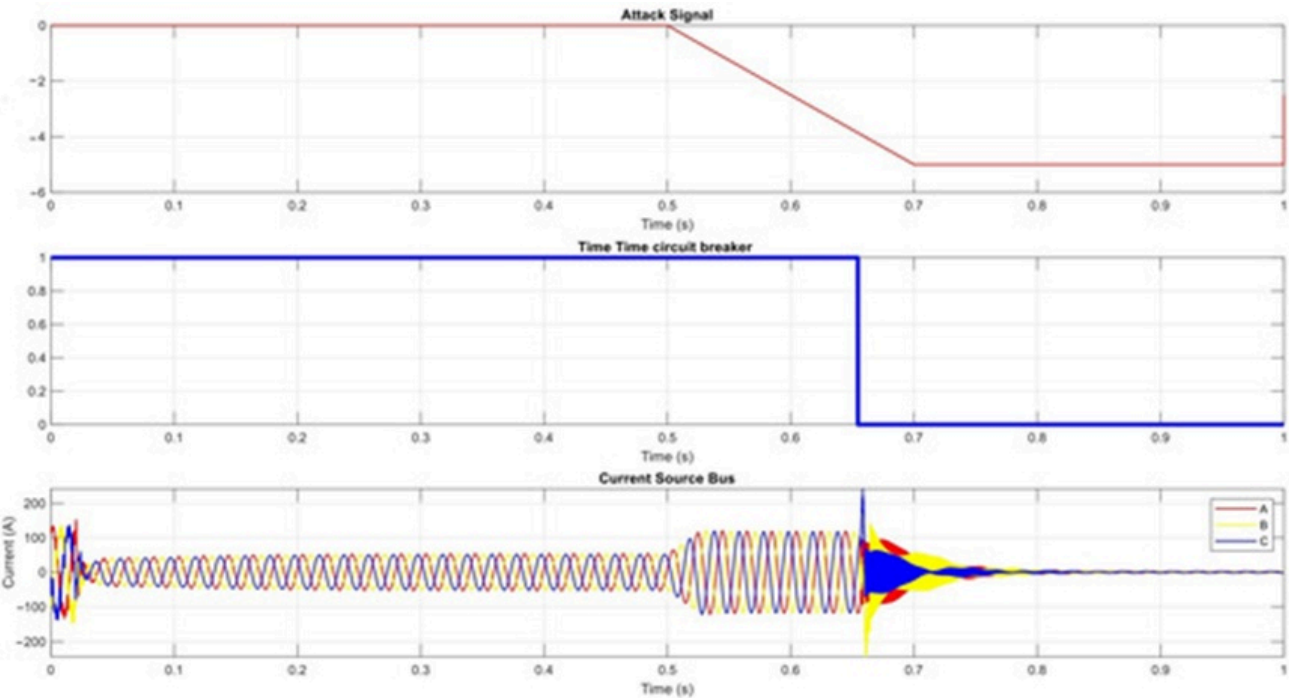


Figure 15. Ramp signal attack applied to the PV inverters.

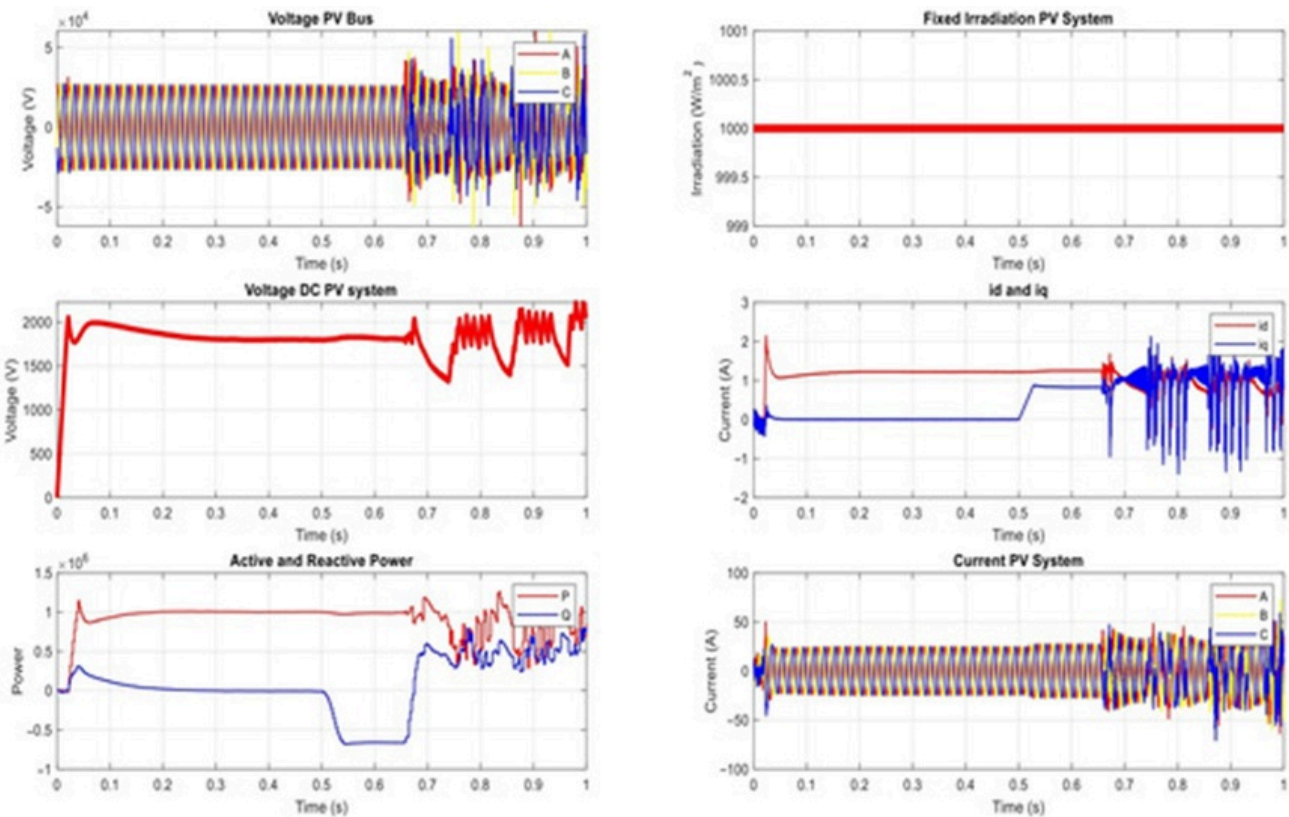


Figure 16. Performance of the proposed power network under a ramp signal attack on the PV inverters.

Overall, this article delivers significant findings and advances in power system protection, intelligent inverters, and cyber-resilience strategies. Accordingly, the present work addresses the key research gaps identified in the existing literature,

as outlined in [Table 1](#). The assessment aligns with the IEC 61850 [\[23\]](#) and GOOSE [\[24\]](#) communication protocols to uncover potential vulnerabilities and limitations in contemporary intelligent power infrastructure.

Furthermore, the study analyzes the transient dynamics of smart PV inverters and OCRs under cyber intrusions, providing an in-depth review of system interactions across multiple attack profiles. To enrich the body of knowledge in this area, a realistic power network is developed using the Electromagnetic Transients Program (EMTP). This approach facilitates the exploration of transient events and dynamic intervals under various grid conditions—ranging from standard operation and steady-state conditions with irradiation reductions to targeted cyberattacks on smart inverters and OCRs during fault occurrences—as summarized in [Table 5](#).

Table 5. Summary of performance outcomes for the proposed power network under manipulating group settings attack on OCR, as well as sine and ramp signal attacks on PV inverters.

A. Performance under manipulated group settings attack on OCR			
Parameter	$t \in [0, 0.5) \text{ s}$	$t \in [0.5, 0.64) \text{ s}$	$t \in [0.64, 1) \text{ s}$
Irradiation	1000 W/m ²	1000 W/m ²	1000 W/m ²
DC Voltage	1800 V	2192 V	random
Active Power	1 MW	Zero	random
Reactive Power	Zero	77.4 var	random
PV AC Current	24.6 A	58.2 A	zero
AC Voltage	25.94 kV	Zero	random
Id (direct-axis current)	1.2 A	1.8 A	random
Iq (quadrature-axis current)	Zero	Zero	random
B. Performance under sine signal attack on PV inverters			
Parameter	$t \in [0, 0.5) \text{ s}$	$t \in [0.5, 0.64) \text{ s}$	$t \in [0.64, 1) \text{ s}$
DC Voltage	1800 V	[1780–1860] V	[1800–2100] V
Active Power	1 MW	[9.5–10.5] MW	[6–8.5] MW
Reactive Power	ZERO	$[(-5)–5] \times 10^5 \text{ var}$	$[3–5] \times 10^5 \text{ var}$
PV AC Current	25 A	35 A	35 A
AC Voltage	26 kV	45 kV	45 kV
Id (direct-axis current)	1.2 A	[1–1.4] A	[0.6–1.6] A
Iq (quadrature-axis current)	Zero	–1.2 / 1.2 A	–1.2 / 1.2 A
C. Performance under ramp signal attack on PV inverters			
Parameter	$t \in [0, 0.5) \text{ s}$	$t \in [0.5, 0.64) \text{ s}$	$t \in [0.64, 1) \text{ s}$
DC Voltage	1800 V	2029 V	Unstable
Active Power	1 MW	1 MW	Unstable
Reactive Power	Zero	–0.66 MW	Unstable

PV AC Current (1-phase)	25.6 A	37.52 A	52 A
AC Voltage	26.5 kV	Unstable	unstable
Id (direct-axis current)	1.2 A	1.2 A	Unstable
Iq (quadrature-axis current)	Zero	0.5 A	Unstable

The control signal attacks (pulse, sine, ramp, and scaling attacks), disrupt grid stability by altering the behavior of reactive power regulation and volt–var control functions. According to the IEEE 1547-2020 standard [5, 15], the volt–var curve enables inverters to regulate grid voltage by injecting or absorbing reactive power up to 44 % of their rated active power capacity. Unintended reactive power flows—whether excessive injection or absorption—can cause under- or overvoltage, leading to operational difficulties and financial consequences. These disturbances elevate the likelihood of damage to circuit components and equipment. When inverters operate in accordance with IEEE 1547 reactive power prioritization, deliberate modification attacks that force extreme reactive power exchange may trigger active power curtailment, resulting in direct revenue losses for the system owner due to reduced active power delivery [28, 29]. Elevated reactive power levels in the network frequently cause voltage instability, which, in turn, creates technical complications and economic impacts while increasing the risk of circuit equipment failure.

Based on the findings and the performance of the currently deployed OCR protection scheme in the modeled network, the majority of cyber attacks directed at the smart inverter level had no discernible effect on the core operating principle of the OCR protection—except in the specific instance of the continuous pulse attack signal. This exception arises because the pulse duration is extremely brief (10 pulses occurring within 0.1 s). Consequently, future enhancements could involve protection strategies that go beyond current magnitude thresholds and incorporate additional indicators such as voltage deviations and harmonic content.

Consistent with the behavior of the implemented OCR protection, most attacks targeting smart inverters left OCR functionality unaffected, except for the pulse signal case. To address this limitation, the study also explores a coordinated cyber-attack scenario in which multiple components (a smart inverter and an OCR) are compromised simultaneously. In this combined attack, a ramp signal is applied to manipulate the reactive power output at the smart inverter. In contrast, a delay attack prevents the trip command from being communicated from the OCR to the circuit breaker after a physical fault is detected, as illustrated in Figure 17. At $t = 0.5$ s, the reactive power injected into the system reached -0.6 MW. The PV system current rose sharply, and the current at the source bus peaked at 100 A. Owing to the simultaneous nature of the coordinated attack, the protection system failed to identify the fault condition and did not initiate corrective action, as evident in Figure 18.

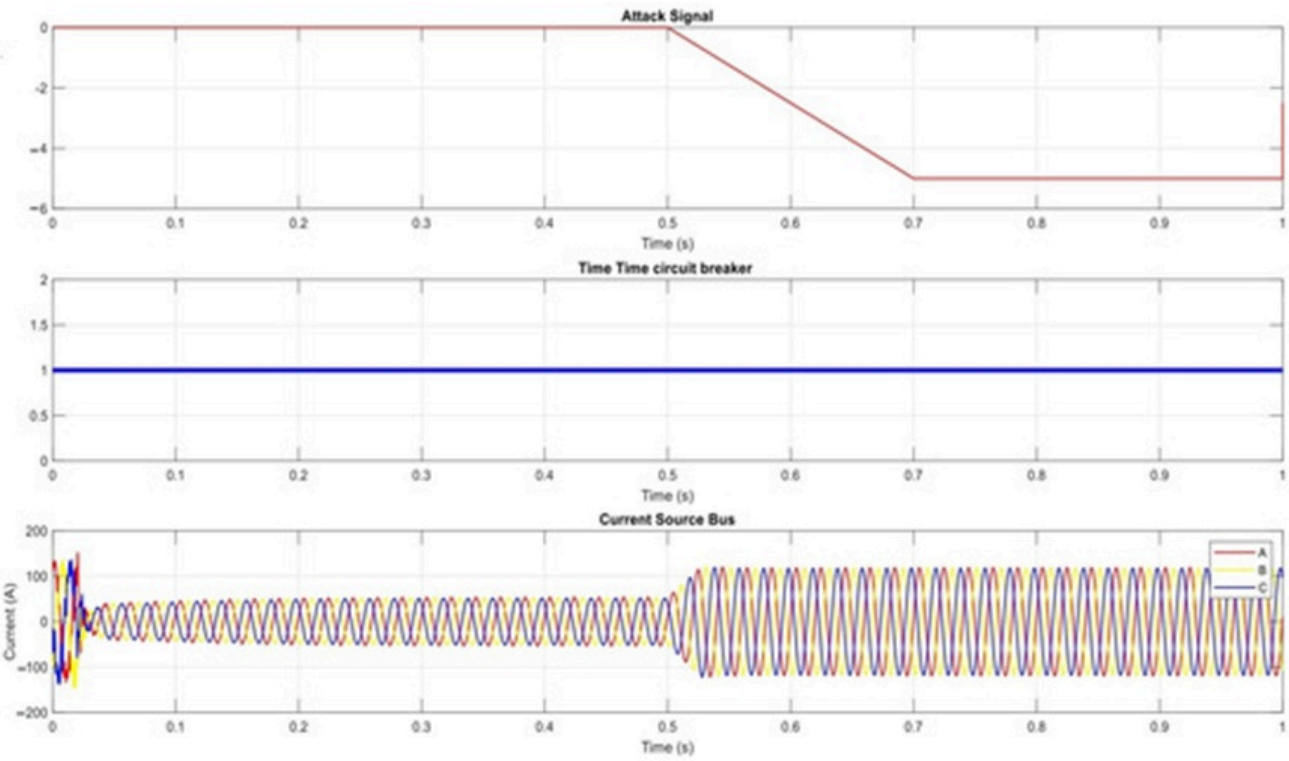


Figure 17. Ramp signal attack on PV inverters combined with circuit breaker delay during a fault condition.

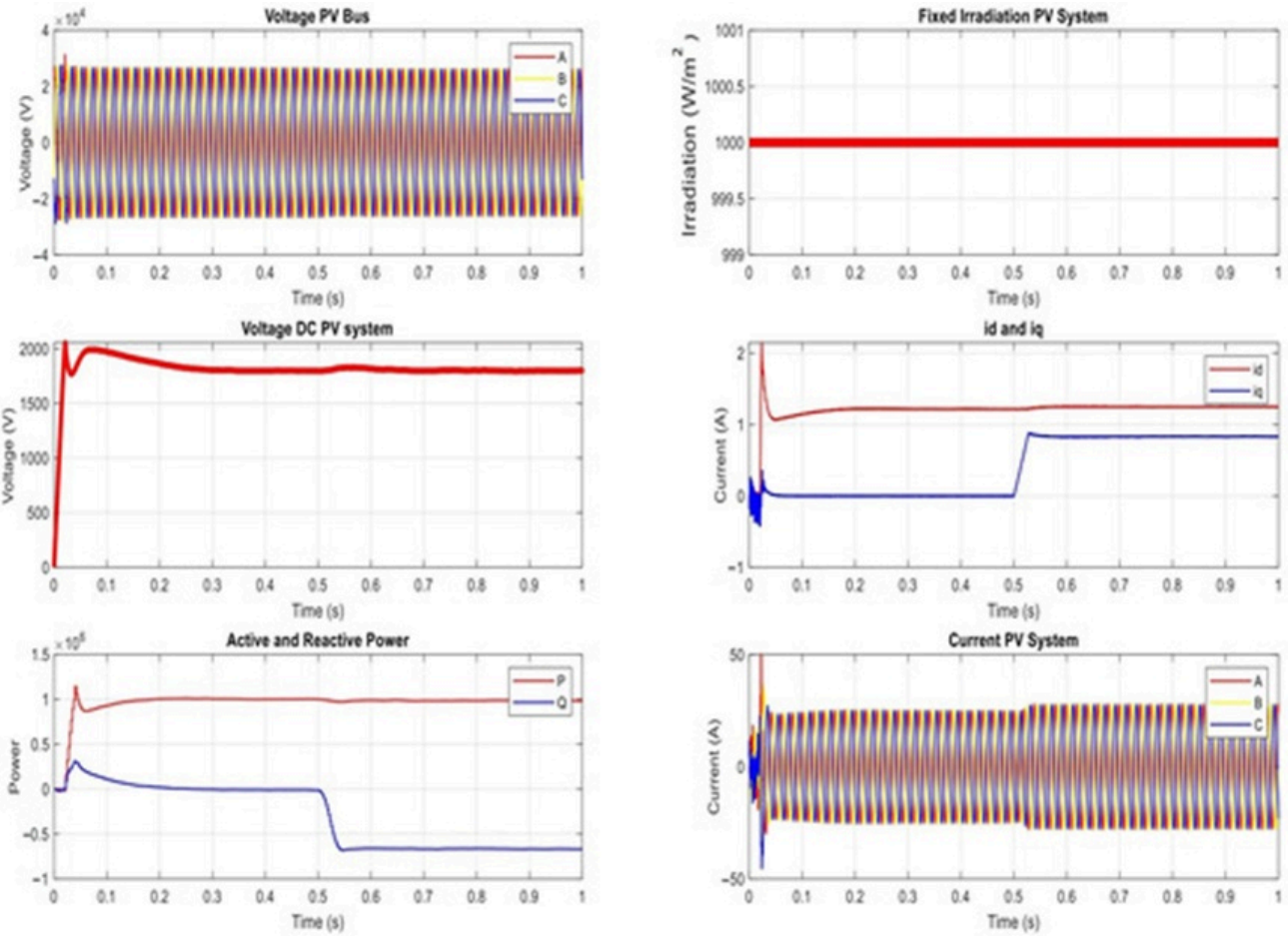


Figure 18. Performance of the proposed power network under a coordinated ramp signal attack on PV inverters and a delay attack on the circuit breaker.

In summary, this investigation—conducted using a realistic network model, simulated conventional faults together with cyber-physical intrusions via the widely adopted EMTP platform, and incorporating OCR characteristics compliant with IEC 255-3 standards [2, 29] as well as smart inverter requirements defined in IEEE 1547-2018 [5, 15]—yields valuable and broadly applicable insights. These standards represent widely accepted benchmarks for inverters and protective relays of various types, thereby allowing the conclusions drawn here to be extended to practical, real-world deployments.

Promising directions for future work include exploring machine learning techniques to improve the detection and classification of cyber intrusions, particularly in power system environments. The integration of machine learning algorithms could substantially strengthen defenses against sophisticated threats and provide more robust cybersecurity safeguards. Another avenue worth pursuing is the design and implementation of a real-time Hardware-in-the-Loop (HIL) testing platform that integrates physical and simulated components. Such an approach would create a more authentic and responsive environment for evaluating the cyber resilience of power systems under live conditions. By pursuing these research pathways, the present study contributes meaningfully to advancing power system security and cyber-resilience practices, ultimately supporting greater reliability and stability in modern electrical grids.

Conclusion

This investigation centers on the escalating challenges arising from integrating Distributed Energy Resources (DERs) with communication infrastructures, particularly in smart inverter control and protective systems. The study underscores the critical threat posed by cyberattacks and their potential to undermine grid stability amid the expanding deployment of grid-connected photovoltaic (PV) installations. Furthermore, the work examines the repercussions of targeted cyber intrusions on key smart grid elements, with special emphasis on smart PV inverters and Overcurrent Relays (OCRs). A thorough analysis of grid modeling and transient responses was performed across multiple cyber-attack scenarios using the Electromagnetic Transients Program (EMTP).

The results shed light on the intricate interdependencies between vulnerabilities in inverters and protection relays, clarifying how the compromise of a single component can propagate widespread effects throughout the system. Additionally, this research assesses the broader implications of cyberattacks on the performance, efficiency, and operational reliability of grid-tied PV systems operating in smart grid environments. As a specific example, during an attack on the PV inverters involving a brief 0.1 s pulse, the OCR was unable to identify the anomaly or isolate the affected section. This failure resulted in elevated current levels reaching 50 A, pronounced harmonic distortion, and substantial power losses, all attributable to the protection scheme's inability to detect and counteract the anomalous attack waveform.

The present study makes a meaningful contribution to understanding cybersecurity vulnerabilities affecting grid-connected solar PV systems. It emphasizes the urgent need to adopt more sophisticated protective mechanisms and enhanced resilience approaches to address the complexities of evolving smart grid architectures. As DER penetration and communication-dependent control continue to advance, a deeper comprehension of cyber threats becomes indispensable. Ultimately, this work plays a vital role in supporting the sustained reliability and robustness of contemporary electrical power networks.

Acknowledgements

We want to thank the Hashemite University (Renewable Energy Center) for its support in publishing this article.

Conflict of interest

None

Financial support

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).

Ethics statement

None

Received: 05 Oct 2023

Revised: 11 Nov 2023

Accepted: 20 Dec 2023

Published online: 20 March 2024

Rights and permissions

Open Access The author(s) retain copyright. This article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. It may be shared and adapted for non-commercial purposes with appropriate attribution, an indication of changes, and distribution of adaptations under the same license. Third-party material may be subject to separate terms identified in its credit line. View the license at <https://creativecommons.org/licenses/by-nc-sa/4.0/>.

References

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. Cham (Switzerland): Springer; 2023.

Brahma SM, Girgis AA. Development of adaptive protection scheme for distribution systems with high penetration of distributed generation. *IEEE Trans Power Deliv*. 2004;19(1):56–63.
<https://doi.org/10.1109/TPWRD.2003.820204>.

Ahmed A, Krishnan VV, Foroutan SA, Touhiduzzaman M, Rublein C, Srivastava A, et al. Cyber physical security analytics for anomalies in transmission protection systems. *IEEE Trans Ind Appl*. 2019;55(6):6313–23.
<https://doi.org/10.1109/TIA.2019.2931278>.

Olowu TO, Dharmasena S, Jafari H, Sarwat A. Investigation of false data injection attacks on smart inverter settings. In: Proceedings of the 2020 IEEE CyberPELS (CyberPELS); 2020 Oct 13; Miami, FL, USA. IEEE; 2020. p. 1–6.
<https://doi.org/10.1109/CyberPELS49534.2020.9311551>.

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); 2023 May 8–11; Wuhan, China. IEEE; 2023. p. 1–7.
<https://doi.org/10.1109/ICPS58381.2023.10128012>.

Yousefi kia M, Saniei M, Seifossadat SG. A novel cyber-attack modelling and detection in overcurrent protection relays based on wavelet signature analysis. *IET Gener Transm Distrib*. 2023;17(7):1585–600.
<https://doi.org/10.1049/gtd2.12783>.

Zhou J, Feng C, Su Q, Jiang S, Fan Z, Ruan J, et al. The multi-objective optimization of powertrain design and energy management strategy for fuel cell–battery electric vehicle. *Sustainability*. 2022;14(10):6320.
<https://doi.org/10.3390/su14106320>.

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.
<https://doi.org/10.1016/j.apenergy.2023.121516>.

Nasirian V, Shafiee Q, Guerrero JM, Lewis FL, Davoudi A. Droop-free distributed control for AC microgrids. *IEEE Trans Power Electron*. 2016;31(2):1600–17.
<https://doi.org/10.1109/TPEL.2015.2455857>.

Rosero CX, 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(8):6461–72.
<https://doi.org/10.1109/TIE.2019.2937039>.

Mahmud MA, Hossain MJ, Pota HR, Oo AMT. Robust nonlinear distributed controller design for active and reactive power sharing in islanded microgrids. *IEEE Trans Energy Convers*. 2014;29(4):893–903.
<https://doi.org/10.1109/TEC.2014.2354826>.

Rey JM, 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(7):1403–15.
<https://doi.org/10.1049/iet-pel.2019.0965>.

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)*; 2022 Sep 5–7; Eindhoven, Netherlands. IEEE; 2022.
<https://doi.org/10.1109/SEST53650.2022.9898440>.

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;10:64397–429.
<https://doi.org/10.1109/ACCESS.2022.3176892>.

Liu X, Li H. Data-driven cyberphysical anomaly detection for microgrids with GFM inverters. *IEEE Open J Power Electron*. 2023;4:498–511.
<https://doi.org/10.1109/OJPEL.2023.3290417>.

Kaewnukultorn T, Sepúlveda-Mora SB, Broadwater R, Zhu D, Tsoutsos NG, Hegedus S. Smart PV inverter cyberattack detection using hardware-in-the-loop test facility. *IEEE Access*. 2023;11:90766–79.
<https://doi.org/10.1109/ACCESS.2023.3307545>.

Bamigbade A, Dvorkin Y, Karri R. Cyberattack on phase-locked loops in inverter-based energy resources. *IEEE Trans Smart Grid*. 2023;14(6):4787–97.
<https://doi.org/10.1109/TSG.2023.3261670>.

Zhang J, Guo L, Ye J, Giani A, Elasser A, Song W, et al. Machine learning-based cyber-attack detection in photovoltaic farms. *IEEE Open J Power Electron*. 2023;4:653–73.
<https://doi.org/10.1109/OJPEL.2023.3304699>.

Piescorovsky EC, Hahn G, Hink RB, 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;10:1099–115.
<https://doi.org/10.1016/j.egyr.2023.07.049>.

Aftab MA, Chawla A, Vergara PP, 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); 2021 Oct 25–28; Aachen, Germany. IEEE; 2021.
<https://doi.org/10.1109/SmartGridComm51999.2021.9632289>.

Rajaei M, Mazlumi K. Multi-agent distributed deep learning algorithm to detect cyber-attacks in distance relays. *IEEE Access*. 2023;11:10842–9.
<https://doi.org/10.1109/ACCESS.2023.3240987>.

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.
<https://doi.org/10.1016/j.ijepes.2023.109062>.

Sowa I, Monti A. Distributed consensus control supported by high reporting rate meters in inverter-based cyber-physical microgrids. *IEEE Access*. 2023;11:48305–21.
<https://doi.org/10.1109/ACCESS.2023.3274570>.

Elrawy MF, Tekki E, Hadjidemetriou L, Laoudias C, Michael MK. 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)*; 2023 Jan 16–19; Washington, DC, USA. IEEE; 2023. p. 1–5.
<https://doi.org/10.1109/ISGT51731.2023.10066452>.

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.
<https://doi.org/10.1016/j.measurement.2023.113678>.

De Oliveira-De Jesus PM, 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.
<https://doi.org/10.1016/j.epsr.2022.108758>.

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.
<https://doi.org/10.1016/j.epsr.2023.109609>.

Pramanik AS, 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(4):1287–303.
<https://doi.org/10.3390/cleantechnol5040064>.

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)*; 2020 Dec 16–19; Jaipur, India. IEEE; 2020.
<https://doi.org/10.1109/PEDES49360.2020.9379880>.