



Cyberattack Detection and Mitigation of False Data Injection in Grid-Connected PV Inverters Using Residual-Based Monitoring and PV-Side Recovery

Amirabbas Homayouni
Zanjan Regional Electric Company

ABSTRACT

The increasing connectivity of photovoltaic (PV) systems and their associated control infrastructures creates new opportunities for cyberattacks that can directly affect inverter operation. This paper investigates a false data injection attack (FDIA) targeting the DC-link voltage measurement of a grid-connected PV inverter. A 250-kW grid-connected PV system implemented in MATLAB/Simulink is considered to examine the effect of the attack on the inverter control response and power conversion performance. A residual-based detection mechanism is developed to identify abnormal changes in the measured DC-link voltage. The residual is monitored against a predefined threshold, and an alarm is generated when the deviation exceeds the threshold. A detection delay is also incorporated into the protection logic to account for the finite time required to activate the recovery action after an attack is detected. Following detection, a PV-side measurement-based recovery mechanism is used to reconstruct the affected voltage signal and provide the inverter controller with a replacement value. The system is evaluated under normal, attack, and recovery conditions. Under the attack scenario, V_{dc_mean} decreases from 481.6 V to 334.6 V, while P_{dc} decreases from 241.5 kW to 177.1 kW and I_{d_ref} reaches 1.5 pu. After the recovery action, V_{dc_mean} returns to approximately 481 V, P_{dc} is restored to 241.5 kW, and I_{d_ref} decreases to 0.9501 pu. The results demonstrate that the considered detection and recovery strategy can effectively reduce the impact of the investigated FDIA on PV inverter operation.

Keywords: PV systems, Cyber-attack, False data injection attack (FDIA), Grid-connected PV inverter, Residual-based detection.

1. INTRODUCTION

Photovoltaic (PV) generation is becoming an increasingly important part of modern power systems, with grid-connected inverters providing the main interface between PV sources and the electrical network. The addition of communication and monitoring functions to these inverters has improved their controllability and integration with the grid, but has also introduced new cyber-physical security concerns [1], [2]. False data injection attacks (FDIAs) are one of the relevant threats in this context. Instead of disrupting a communication link directly, an attacker can manipulate measurement data and allow the modified information to continue through the control system. Studies on distributed energy resources and smart inverters have shown that such manipulation can influence inverter settings and coordinated control actions, linking the integrity of digital measurements to the physical behavior of the power system [3], [4].

For PV systems, the consequences can be particularly important when the compromised measurement is used directly by the inverter controller. An abnormal measurement may cause the controller to modify its operating point even though the electrical equipment itself has not experienced a corresponding physical disturbance. This makes the identification of abnormal measurements an important step in limiting the propagation of a cyberattack into the physical layer. Several detection approaches have consequently been investigated for inverter-based resources [6]. These include data-driven techniques as well as methods that exploit physical characteristics or measurements available within the system. The use of locally available information is especially relevant when communication-based information cannot be assumed to be trustworthy, and previous work has investigated physical-invariant and measurement-based approaches for detecting or mitigating attacks on smart inverters [5].



Detection, however, does not necessarily eliminate the effect of a compromised signal. If the affected measurement remains connected to the control loop after an alarm is generated, the controller can continue responding to incorrect information until a recovery action is applied. The time required to detect the attack and activate this action can therefore influence the transient response and the final operating condition.

In this work, an FDIA is considered at the DC-link voltage measurement of a grid-connected PV inverter. The study is carried out using the 250-kW grid-connected PV array model implemented in MATLAB/Simulink. The attack modifies the voltage measurement supplied to the inverter control system, and its effect is examined through the resulting changes in the DC-link voltage, DC power, and current reference. A residual-based monitoring mechanism is first employed to identify the abnormal measurement. After detection, a PV-side measurement-based recovery mechanism is used to provide a replacement value for the affected signal under the considered single-channel attack assumption. The response of the system is then compared in normal, attacked, and recovered conditions, while the detection and recovery delay is also considered in the evaluation. This provides a combined assessment of the detection and mitigation response rather than evaluating the attack detector independently from the subsequent recovery action.

2. SYSTEM DESCRIPTION

The system considered in this study is the 250-kW grid-connected PV array model implemented in MATLAB/Simulink. The model represents a grid-connected photovoltaic generation unit in which the PV array supplies DC power to a voltage-source inverter, while the inverter control system regulates the conversion of the generated power to the AC side. The DC-link voltage is an important variable in this process because it is directly associated with the operating condition of the power conversion stage.

The PV array and inverter are connected through the DC-link, where the DC voltage is measured and supplied to the control system. The measured voltage, denoted as V_{dc_meas} , is used by the inverter control structure to determine its operating response. Other variables, including the PV-side DC voltage and power, are also available within the model and are used later in this study as supporting information for the recovery mechanism.

To investigate the cyber-physical effect of a measurement attack, the communication path associated with the DC-link voltage measurement is considered the attack surface. A false value is injected into the V_{dc_meas} signal before it reaches the inverter control system. Therefore, the electrical connection of the PV array and inverter is not physically modified by the attack; instead, the controller receives an altered representation of the DC-link voltage and reacts according to the corrupted measurement.

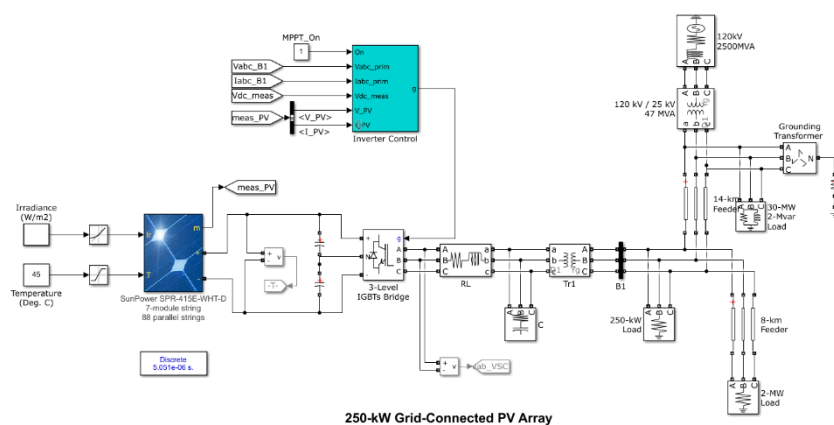


Fig. 1. Simplified structure of the 250-kW grid-connected PV system and the considered cyber-attack path

The study assumes a single-channel false data injection scenario in which the DC-link voltage measurement is compromised while the PV-side measurements used for the recovery process remain available. This assumption defines the scope of the present study and allows the effect of a compromised control-loop measurement to be examined independently. More comprehensive multi-channel attacks, in which both the



inverter-side and PV-side measurements are simultaneously compromised, are outside the scope of this work and are considered as a potential direction for future investigation.

3. THREAT MODEL AND ATTACK SCENARIO

The considered threat model assumes that the PV inverter is connected to a communication network through which measurement and control information can be exchanged. This connectivity provides a potential entry point for an attacker who has obtained access to the inverter communication path. The objective of the attacker is not to interrupt the communication channel, but to alter the information received by the inverter control system.

In the considered scenario, the attacker targets the DC-link voltage measurement V_{dc_meas} . A false value is introduced into this signal before it reaches the corresponding control block, while the physical DC-link voltage remains unaffected at the instant of data manipulation. This type of attack represents a false data injection condition in which the controller operates on information that does not correctly represent the actual electrical state of the system [3], [6].

The attack is applied to a single measurement channel. The remaining PV-side measurements are assumed to remain available during the considered attack and are subsequently used as supporting information for the recovery process. This assumption is intentionally limited to a single-channel compromise so that the response of the inverter to an individual corrupted measurement can be isolated and evaluated. Multi-channel attacks involving simultaneous manipulation of the PV-side measurements are not considered in the present study.

The false data injection attack is modeled by adding an artificial DC component to the measured DC-link voltage. As a result, the voltage signal received by the inverter controller differs from the actual measured value. The attacked voltage signal is expressed as:

$$V_{dc_attacked}(t) = V_{dc_meas}(t) + \Delta V_{attack}(t) \quad (1)$$

where $V_{dc_meas}(t)$ represents the measured DC-link voltage, $\Delta V_{attack}(t)$ denotes the injected false voltage component, and $V_{dc_attacked}(t)$ is the corrupted voltage signal applied to the inverter control system. During the attack interval, $\Delta V_{attack}(t)$ is activated and increases the reported voltage seen by the controller. The magnitude of the injected component is selected such that the resulting abnormal measurement can drive the inverter toward an undesired operating condition and, depending on the selected attack level, may lead to the activation of overvoltage protection. The term $\Delta V_{attack}(t)$ can be defined according to the temporal profile of the attack:

A. Abrupt False Data Injection: In the primary simulation scenario, the false data is introduced as an abrupt change in the DC-link voltage measurement. In this case, the attacker suddenly modifies the measured voltage by injecting a predefined voltage component at the attack initiation time.

B. Ramp-Type False Data Injection: The attack model is not limited to an abrupt change in the measured DC-link voltage. A gradual or ramp-type manipulation can also be represented, in which the injected voltage component increases progressively after the attack begins. This allows the considered threat model to cover both abrupt and progressively developing measurement attacks.

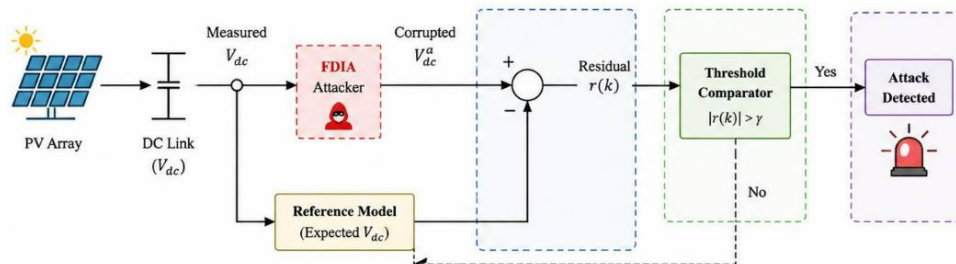


Fig. 2. Considered false data injection attack on the DC-link voltage measurement path

To evaluate the physical impact of the attack, the manipulated V_{dc_meas} signal is supplied to the inverter control structure during the attack interval. The resulting change in the controller response is observed through the DC-link operating condition, the DC power P_{dc} , and the inverter current reference I_{d_ref} . Previous



investigations of cyberattacks on distributed energy resources and inverter-based systems have similarly shown that manipulation of measurement or control information can propagate from the cyber layer to the physical operating response [4], [7].

The attack scenario is evaluated in three operating conditions. First, the system is operated without an attack to establish the normal operating response. The attack is then activated by modifying the DC-link voltage measurement, allowing the resulting deviation in the inverter response to be observed. Finally, after the attack is detected, the recovery mechanism is activated and the resulting operating condition is compared with the normal and attacked cases.

The objective of this scenario is therefore not to reproduce every possible cyberattack against a PV inverter, but to provide a controlled test case for examining the complete sequence of measurement manipulation, attack detection, and signal recovery. This approach also provides a consistent basis for evaluating the effectiveness of the proposed recovery mechanism using the same inverter and operating conditions throughout the study.

4. RESIDUAL-BASED ATTACK DETECTION

Different FDIA detection approaches have been investigated for renewable-rich power systems, including data-driven methods designed to address uncertainties associated with high renewable penetration [8]. For grid-connected PV inverters, data-driven detection approaches based on CNN and LSTM architectures have also been investigated for identifying cyberattacks [9]. The cybersecurity of smart inverters has received increasing attention because their communication capabilities and grid-support functions introduce additional cyberattack exposure [10]. Previous studies have considered a broad range of cyberattacks against inverter-based power systems together with corresponding detection and mitigation strategies [11]. The detection mechanism is based on the deviation between the voltage measurement used by the inverter controller and a reference value representing the expected DC-link voltage [6]. This deviation is expressed as a residual, which provides a simple indicator of abnormal changes in the measured signal. The residual is calculated as:

$$r(t) = |V_{dc_meas}(t) - V_{dc_mean}(t)| \quad (2)$$

where $V_{dc_meas}(t)$ is the voltage measurement supplied to the inverter control system and $V_{dc_mean}(t)$ represents the corresponding expected voltage level obtained from the available PV-side information. Under normal operating conditions, the two signals remain close to each other and the residual is therefore relatively small. When false data is injected into the voltage measurement, the difference increases and provides an indication of a possible attack. A threshold-based decision rule is adopted for attack detection:

$$\begin{aligned} \text{Alarm}(t) &= 1, & \text{if } r(t) > T \\ \text{Alarm}(t) &= 0, & \text{otherwise.} \end{aligned} \quad (3)$$

The detection threshold T is selected based on statistical analysis of the residual under normal operating conditions, specifically:

$$T = \mu_r + 3\sigma_r \quad (4)$$

where μ_r and σ_r are the mean and standard deviation of the residual during steady-state operation without attack. This 3σ criterion ensures a false alarm probability below 0.3% while maintaining fast detection of FDIAs that inject deviations exceeding this statistical bound.

To avoid undesired alarm activations during the initial simulation transient, a time-based activation condition is incorporated into the detection logic, preventing false detections caused by startup dynamics. When the residual exceeds the threshold, the alarm changes from zero to one and indicates that the measured DC-link voltage should no longer be considered suitable for direct use by the subsequent recovery stage. The alarm signal is consequently used as the decision variable for activating the mitigation process. The finite response time between the appearance of the abnormal measurement and the activation of the recovery path is retained in the simulation to evaluate its effect on the inverter response.

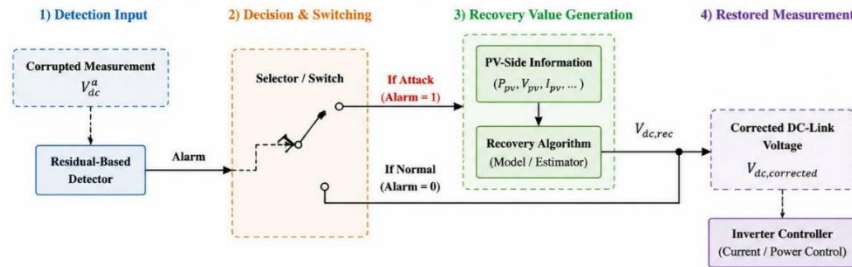


Fig. 3. Residual-based detection mechanism and alarm generation for the considered false data injection attack.

Under normal conditions, the residual remains below the selected threshold and the alarm remains inactive. Once the injected false data produces a sufficiently large deviation, the residual crosses the threshold and the alarm is activated. This provides the transition from the detection stage to the recovery stage investigated in the following section. FDIA detection has also been investigated in distribution-level power systems, demonstrating that measurement manipulation can be considered across different levels of the power-system architecture [12].

5. RESIDUAL-BASED ATTACK DETECTION

For grid-connected solar PV systems, the cybersecurity of intelligent inverters must account for both their control functions and their associated communication capabilities [13]. Once the residual-based detector identifies an abnormal condition, the corrupted DC-link voltage measurement should no longer be directly applied to the inverter control loop. The recovery stage therefore uses the detection alarm as the decision signal for changing the input provided to the controller. Under normal conditions, the measured voltage is retained, whereas after attack detection, the recovery path is activated.

The replacement signal is obtained from the available PV-side information. This approach does not require the physical DC-link voltage to be directly measured by an additional sensor at the point affected by the attack. Instead, the available information on the source side is used to construct a suitable replacement for the compromised measurement. The underlying assumption is that the considered attack affects only the DC-link voltage measurement channel and does not simultaneously compromise the PV-side measurements.

The transition between the original and recovery signals is controlled by the alarm state. When the alarm remains inactive, the original measurement continues to the inverter controller. Once the alarm becomes active, the recovery value is selected instead. In this way, the recovery mechanism can be represented conceptually as:

$$\begin{aligned} V_{dc_corrected}(t) &= V_{dc_meas}(t), & \text{if Alarm}(t) = 0 \\ V_{dc_corrected}(t) &= V_{dc_recovery}(t), & \text{if Alarm}(t) = 1 \end{aligned} \quad (5)$$

Where $V_{dc_corrected}$ is the signal supplied to the inverter control system and $V_{dc_recovery}$ represents the replacement value obtained from the PV-side information. The switching decision is based on the detection result rather than on a direct comparison with a predefined attacked-voltage value.

A finite delay is retained between the detection of the abnormal condition and the effective activation of the recovery path. Consequently, the corrupted signal can affect the inverter response for a short period after the attack begins. Including this delay makes it possible to evaluate not only the steady-state recovery performance but also the transient effect associated with the detection and recovery process. The effectiveness of the recovery mechanism is evaluated by comparing the inverter response before the attack, during the attack, and after recovery. Particular attention is given to V_{dc_mean} , P_{dc} , and I_{d_ref} , since changes in these quantities directly reflect the effect of the corrupted measurement on the inverter operating condition. A successful recovery is therefore considered when the affected operating variables return close to their corresponding normal-condition values after activation of the recovery path. PV cybersecurity therefore requires mitigation strategies that consider the interaction between cyber threats and the physical behavior of the photovoltaic system [14].



6. RESULTS AND DISCUSSION

The cybersecurity of smart inverters has become an important research topic because their increasing communication and grid-support capabilities introduce additional cyberattack exposure [10]. Existing research on inverter-based smart power systems has considered a range of cyberattacks together with corresponding detection and mitigation strategies [11]. The performance of the considered detection and recovery scheme is evaluated under three operating conditions: normal operation, attack condition, and recovery after attack detection. The same 250-kW grid-connected PV system is used for all three cases to provide a consistent basis for comparison. The main variables considered in the evaluation are V_{dc_mean} , P_{dc} , I_{d_ref} , V_{dc_meas} , and the generated alarm signal.

A. Normal Operating Condition

The first case represents the normal operation of the PV system without any cyberattack. The inverter operates under its nominal control conditions, and the monitored variables remain within their expected operating range. The corresponding values obtained from the simulation are $V_{dc_mean}=481.6$ V, $P_{dc}=241.5$ kW, and $I_{d_ref}=0.9606$ pu.

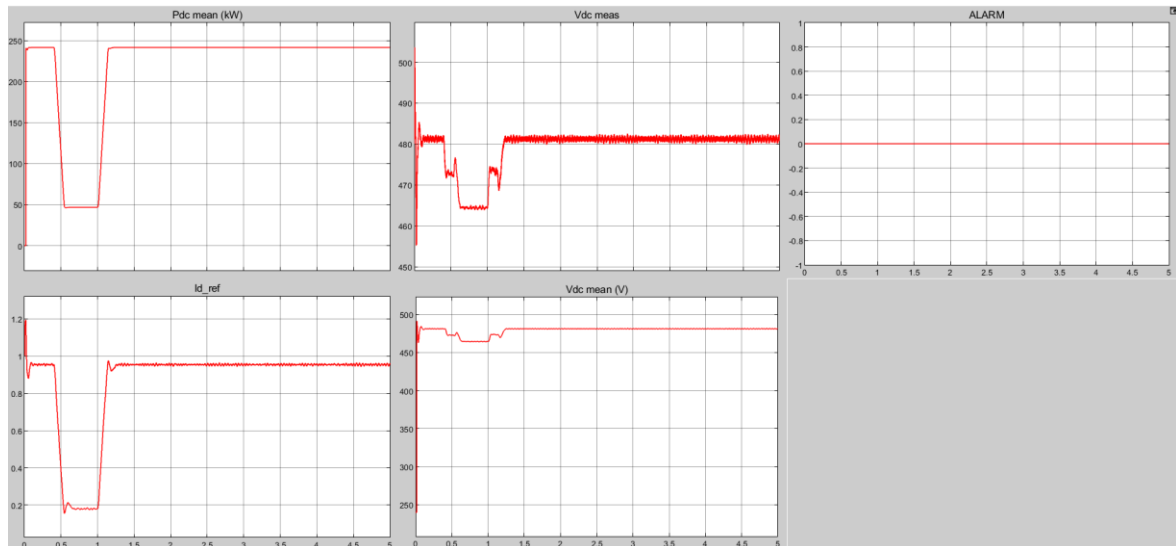


Fig. 4. Simulation results under normal operating conditions, including the alarm signal, P_{dc} , I_{d_ref} , V_{dc_meas} , and V_{dc_mean} .

The alarm remains inactive during this condition, indicating that the residual does not reach the level required to trigger the detection mechanism. These results establish the baseline against which the effects of the false data injection attack and the subsequent recovery are evaluated.

B. Attack Condition and Detection Response

In the second case, the false data injection attack is activated on the DC-link voltage measurement. The manipulated measurement is supplied to the inverter control system, causing the controller to operate based on incorrect voltage information. The effect of this manipulation can be observed in the monitored electrical variables as well as in the alarm response.

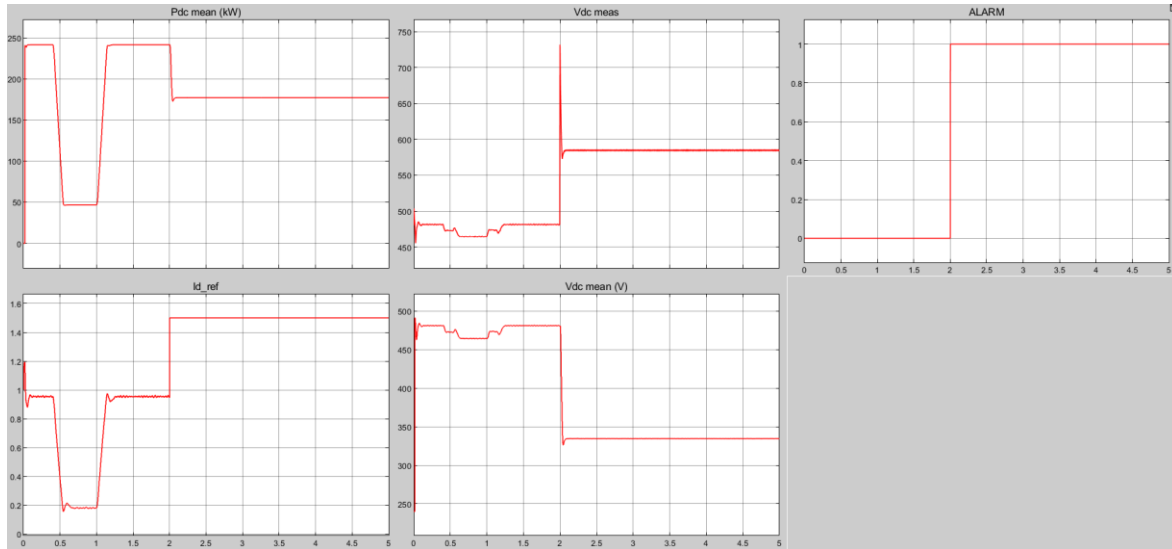


Fig. 5. Simulation results during the false data injection attack and residual-based detection.

During the attack, V_{dc_mean} decreases from 481.6 V to 334.6 V. At the same time, P_{dc} decreases from 241.5 kW to 177.1 kW, while I_{d_ref} increases from 0.9606 pu and reaches 1.5 pu. The current reference therefore reaches the considered upper operating limit while the available DC power is substantially reduced. The alarm signal changes to one after the abnormal condition is detected, providing the trigger for the recovery stage.

To quantify the magnitude of the deviation introduced by the attack, the percentage deviation from the normal operating value is calculated as:

$$\text{Attack Deviation (\%)} = (|X_{\text{attack}} - X_{\text{normal}}| / X_{\text{normal}}) \times 100 \quad (6)$$

where X represents the parameter under consideration. Based on (6), the attack produces a 30.52% deviation in V_{dc_mean} , a 26.67% deviation in P_{dc} , and a 56.15% deviation in I_{d_ref} relative to their normal operating values.

The simulation also shows that detection and recovery are not instantaneous. A short transient interval occurs between the appearance of the abnormal measurement, activation of the alarm, and effective operation of the recovery path. This interval is retained in the evaluation because it represents an important part of the practical response of the proposed mitigation process.

C. Recovery Condition

After the attack is detected, the recovery mechanism is activated and the corrupted measurement is replaced by the recovery signal described in Section V. The purpose of this stage is to prevent the attacked measurement from continuing to drive the inverter controller and to restore the operating variables toward their pre-attack values.

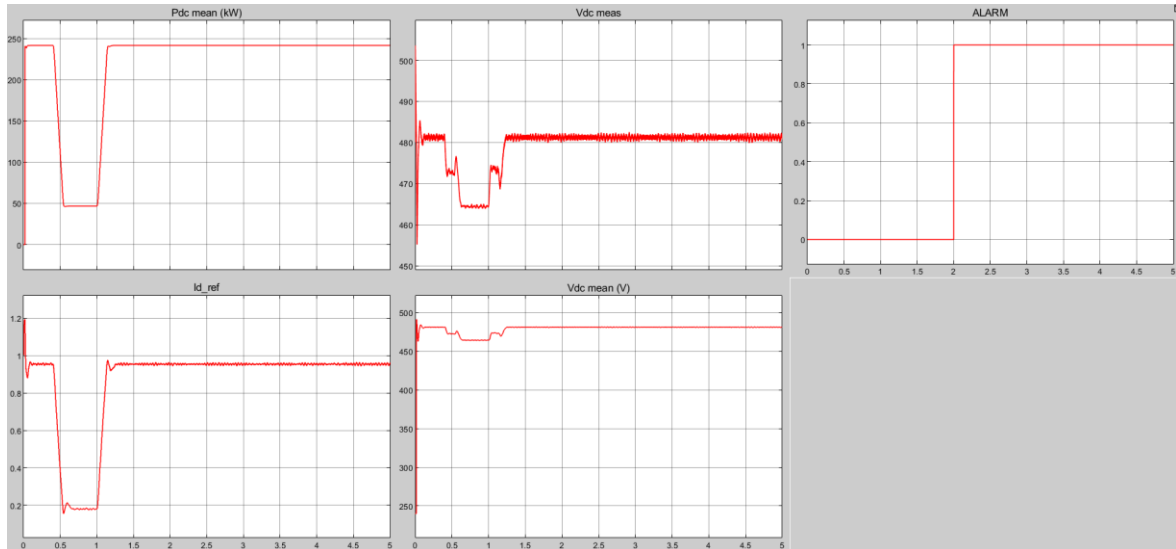


Fig. 6. Simulation results after activation of the recovery mechanism.

The recovery response shows a clear return toward the normal operating condition. V_{dc_mean} increases from the attacked value of 334.6 V to approximately 481 V, while P_{dc} returns to 241.5 kW. The I_{d_ref} value also decreases from the 1.5-pu level observed during the attack to 0.9501 pu, which is close to the normal value of 0.9606 pu.

The remaining error after recovery is evaluated with respect to the normal operating value using:

$$\text{Recovery Error (\%)} = (|X_{\text{recovery}} - X_{\text{normal}}| / X_{\text{normal}}) \times 100 \quad (7)$$

Using (7), the remaining error in V_{dc_mean} is 0.12%, while the recovery error for P_{dc} is 0.00%. For I_{d_ref} , the remaining error is 1.09%. These values indicate that the main operating variables return very close to their corresponding pre-attack values after activation of the recovery mechanism.

D. Quantitative Comparison

A quantitative comparison of the three operating conditions is presented in Table 1. The results show a clear distinction between normal, attacked, and recovered operation. The attack produces substantial deviations in all three principal performance variables, whereas the recovery stage significantly reduces these deviations.

Table 1. Comparison of System Response Under Normal, Attack, and Recovery Conditions

Parameter	Normal	Attack	Recovery	Attack Deviation (%)	Recovery Error (%)
V_{dc_mean} (V)	481.6	334.6	481.0	30.52	0.12
P_{dc} (kW)	241.5	177.1	241.5	26.67	0.00
I_{d_ref} (pu)	0.9606	1.5000	0.9501	56.15	1.09

The quantitative results provide two important observations. First, the false data injection attack is able to propagate from the compromised measurement into the physical operating response of the PV inverter. The 30.52% deviation in V_{dc_mean} and 26.67% deviation in P_{dc} demonstrate the effect of the manipulated measurement on the operating condition, while the 56.15% deviation in I_{d_ref} shows a more pronounced response in the inverter current reference.

Second, the recovery mechanism substantially reduces the deviation produced by the attack. The DC power returns to exactly its normal value, and the remaining errors in V_{dc_mean} and I_{d_ref} are limited to 0.12% and 1.09%, respectively. Therefore, within the single-channel attack scenario considered in this study, the proposed detection and recovery sequence is able to restore the main operating variables to values close to their normal condition.



It is worth noting that the proposed recovery mechanism is also resilient against gradual false data injection attacks. Also it should be emphasized that these results are specific to the considered attack scenario and the assumption that the PV-side information used by the recovery mechanism remains uncompromised. The results should therefore not be interpreted as a general guarantee against attacks involving simultaneous manipulation of multiple measurement channels. Such scenarios require a more comprehensive recovery architecture and are left for future investigation.

7. CONCLUSION AND FUTURE WORK

This paper investigated the cyber-physical impact of a false data injection attack targeting the DC-link voltage measurement of a grid-connected PV inverter. Using a 250-kW PV system implemented in MATLAB/Simulink, the study considered the complete sequence from measurement manipulation and residual-based detection to post-detection recovery. The results show that compromising a single voltage measurement can noticeably affect the operating response of the inverter.

Under the considered attack condition, V_{dc_mean} decreased from 481.6 V to 334.6 V, while P_{dc} decreased from 241.5 kW to 177.1 kW. At the same time, I_{d_ref} increased from 0.9606 pu to 1.5 pu. After the recovery mechanism was activated, V_{dc_mean} returned to approximately 481 V and P_{dc} recovered to 241.5 kW, while I_{d_ref} decreased to 0.9501 pu. The corresponding recovery errors were 0.12%, 0.00%, and 1.09% for V_{dc_mean} , P_{dc} , and I_{d_ref} , respectively.

The results demonstrate that the considered residual-based detection and PV-side measurement-based recovery strategy can effectively reduce the operational impact of the investigated single-channel FDIA. However, the recovery process relies on the availability and integrity of the PV-side information used to reconstruct the affected signal. Therefore, the presented results should be interpreted within the attack assumptions defined in this study rather than as a general solution for all possible measurement attacks. Future work will focus on developing a more independent recovery architecture that does not rely on a single assumed-trusted measurement path. In particular, analytical redundancy, multiple heterogeneous measurements, model-based reconstruction, and digital-twin-based estimation can be investigated to provide an additional layer of resilience when several measurements may be compromised simultaneously. Extending the proposed framework to coordinated multi-channel attacks and evaluating its performance under different operating conditions will also be considered. Future extensions should consider coordinated attacks involving multiple DER measurements and communication channels, since the increasing interconnection and controllability of DERs can expand the potential cyberattack surface [15].

REFERENCES

- [1] Albusnashee, Hamdi M., Chris Farnell, Andrew Suchanek, Kelby Haulmark, Roy A. McCann, Jia Di, and Alan Mantooth. "A test bed for detecting false data injection attacks in systems with distributed energy resources." *IEEE Journal of Emerging and Selected Topics in Power Electronics* 10, no. 1 (2019): 1303-1315.
- [2] Jhala, Kumarsinh, Parth Pradhan, and Balasubramaniam Natarajan. "Perturbation-based diagnosis of false data injection attack using distributed energy resources." *IEEE Transactions on Smart Grid* 12, no. 2 (2020): 1589-1601.
- [3] Olowu, Temitayo O., Shamini Dharmasena, Hassan Jafari, and Arif Sarwat. "Investigation of false data injection attacks on smart inverter settings." In *2020 IEEE CyberPELS (CyberPELS)*, pp. 1-6. IEEE, 2020.
- [4] Jafarigiv, Danial, Keyhan Sheshyekani, Marthe Kassouf, Younes Seyedi, Houshang Karimi, and Jean Mahseredjian. "Countering FDI attacks on DERs coordinated control system using FMI-compatible cosimulation." *IEEE Transactions on Smart Grid* 12, no. 2 (2020): 1640-1650.
- [5] Khan, Mohammed Ali, VS Bharath Kurukuru, Subham Sahoo, and Frede Blaabjerg. "From physics to data oriented cyber attack profile emulation in grid connected PV systems." In *2021 IEEE 22nd Workshop on Control and Modelling of Power Electronics (COMPEL)*, pp. 1-8. IEEE, 2021.
- [6] Riggs, Hugo, Shahid Tufail, Mohammad Khan, Imtiaz Parvez, and Arif I. Sarwat. "Detection of false data injection of PV production." In *2021 IEEE Green Technologies Conference (GreenTech)*, pp. 7-12. IEEE, 2021.
- [7] Kumaresan, Anusha, Nandha Kumar Kandasamy, and Robert E. Kooij. "Edge security in smart



- inverters: Physical invariants based approach.*" *International Journal of Electrical Power & Energy Systems* 141 (2022): 108039.
- [8] Mohammadpourfard, Mostafa, Yang Weng, Istemihan Genc, and Taesic Kim. "An accurate false data injection attack (FDIA) detection in renewable-rich power grids." In *2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, pp. 1-5. IEEE, 2022.
- [9] Mao, Jiaying, Mengfan Zhang, and Qianwen Xu. "CNN and LSTM based Data-driven Cyberattack Detection for Grid-connected PV Inverter." In *2022 IEEE 17th international conference on control & automation (ICCA)*, pp. 704-709. IEEE, 2022.
- [10] Li, Yuanliang, and Jun Yan. "Cybersecurity of smart inverters in the smart grid: A survey." *IEEE Transactions on Power Electronics* 38, no. 2 (2022): 2364-2383.
- [11] Tuyen, Nguyen Duc, Nguyen Sy Quan, Vo Ba Linh, Vu Van Tuyen, and Goro Fujita. "A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy." *Ieee Access* 10 (2022): 35846-35875.
- [12] Radoglou-Grammatikis, Panagiotis, Christos Dalamagkas, Thomas Lagkas, Magda Zafeiropoulou, Maria Atanasova, Pencho Zlatev, Alexandros-Apostolos A. Boulogeorgos et al. "False data injection attacks against low voltage distribution systems." In *GLOBECOM 2022-2022 IEEE Global Communications Conference*, pp. 1856-1861. IEEE, 2022.
- [13] Vodapally, Sai Nikhil, and Mohd Hasan Ali. "Overview of intelligent inverters and associated cybersecurity issues for a grid-connected solar photovoltaic system." *Energies* 16, no. 16 (2023): 5904.
- [14] Harrou, Fouzi, Bilal Taghezouit, Benamar Bouyeddou, and Ying Sun. "Cybersecurity of photovoltaic systems: challenges, threats, and mitigation strategies: a short survey." *Frontiers in Energy Research* 11 (2023): 1274451.
- [15] Zografopoulos, Ioannis, Nikos D. Hatziaegyriou, and Charalambos Konstantinou. "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations." *IEEE Systems Journal* 17, no. 4 (2023): 6695-6709.