ReThink: Reveal the Threat of Electromagnetic Interference on Power Inverters

Fengchen Yang[1,2*], Zihao Dan[1,2*], Kaikai Pan[1,2†], Chen Yan[1,2], Xiaoyu Ji[1,2], and Wenyuan Xu[1,2]
[1] Zhejiang University
[2] ZJU QI-ANXIN IoT Security Joint Labratory
{yangfengchen, danzihao, pankaikai, yanchen, xji, wyxu}@zju.edu.cn

***Abstract*—With the boom of renewable energy sources (RES), the number of power inverters proliferates. Power inverters are the key electronic devices that transform the direct current (DC) power from RES to the alternating current (AC) power on the grids, and their security can affect the stable operation of RES and even power grids. This paper analyzes the security of photovoltaic (PV) inverters from the aspects of internal sensors since they serve as the foundation for safe power conversion. We discover that both the embedded current sensors and voltage sensors are vulnerable to electromagnetic interference (EMI) of 1 GHz or higher, despite electromagnetic compatibility (EMC) countermeasures. Such vulnerabilities can lead to incorrect measurements and deceiving the control algorithms, and we design ReThink that could produce three types of consequences on PV inverters by emitting carefully crafted EMI, i.e., Denial of Service (DoS), damaging inverters physically or damping the power output. We successfully validate these consequences on 5 off-the-shelf PV inverters, and even in a real-world microgrid, by transmitting EMI signals at a distance of $100 \sim 150$cm and a total power within 20 W. Our work aims to raise awareness of the security of power electronic devices of RES, as they represent an emerging Cyber-Physical attack surface to the future RES-dominated grid. Finally, to cope with such threats, we provide hardware and software-based countermeasures.**

I. Introduction

Renewable energy sources (RES), e.g., solar, wind, or hydroelectric power, are replacing fossil fuels to reduce their impact on global climate change [54] and are expected to account for 47.7% of all energy sources by 2040 [59]. As the penetration rate of RES continues to increase, it is critical to examine the emerging security issues of the power grids before RES constructions are finalized. Since most RES generates direct current (DC) power, yet the grids and power consumers operate on alternating current (AC) power, millions of power inverters have to be installed to convert DC power into AC power for each RES, as shown in Fig. 1. Thus, the security of power inverters can affect the smooth operation of RES power generation and even the stability of the power grids. Without loss of generality, we perform a systematic security analysis of solar inverter, aka., photovoltaic (PV) inverter, with the goal of providing security insights to device developers and designers, since PV is one of the most important RES and its capacity will produce about one-third of the world's annual energy consumption by 2050 [18], [70].

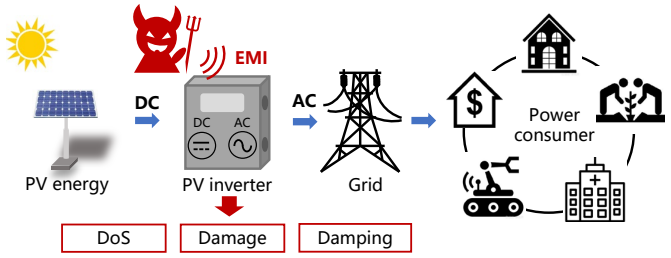


Fig. 1. An illustration of ReThink: EMI can affect PV inverters and cause DoS or physical damage, or damping the power output.

In this paper, we focus on the distinct security of inverters, i.e., the security of analog sensors, since inverters rely on correct sensing of voltage and current of input power sources as well as the grids to ensure stable and safe power conversion. For instance, without accurate sensing of current and voltage, the inverter may fail to detect islanding conditions (when the grid is down but the inverter is still producing power) and potentially cause fire or electrify a maintenance technician [91]. Sensors are known to be vulnerable to electromagnetic interference (EMI) [67], [14], [43], [83], and most PV inverters are installed in unguarded areas, e.g., resident backyards, building rooftops, or power plants in a desert [60], whereby immersing sensors with malicious EMI signals is possible.

These observations motivate us to perform further investigation into the impact of EMI on PV inverters, yet the DC-AC power conversion circuits inside inverters generally handle 50 watts up to 50 kilowatts [19] and are a natural and strong source of EMI by design. For instance, power semiconductor switches that commutate at high switching frequencies will radiate EMI. Thus, all power inverters have to satisfy the electromagnetic compatibility (EMC) requirements by properly grounding, adding filters, and shielding so that they can operate normally in the presence of self and mutual interference. Although prior work [6] has shown that static magnetic field can affect Hall sensors at a distance of 10 cm, it is unclear whether EMI injection could affect other types of embedded sensors, e.g., voltage sensors, and whether EMI signals can be crafted to precisely manipulate chosen sensors, as well as their consequences on inverters as a whole.

After performing a systematic security analysis of the PV

* Fengchen and Zihao contributed equally to this work.
† Kaikai Pan is the corresponding author.

Network and Distributed System Security (NDSS) Symposium 2025
24-28 February 2025, San Diego, CA, USA
ISBN 979-8-9894372-8-3
https://dx.doi.org/10.14722/ndss.2025.230691
www.ndss-symposium.org

inverters on real inverters and microgrid [1], we discover that both the embedded current and voltage sensors in PV inverters are vulnerable to EMI, *although they conform to EMC standards on conduction and radiation interference* [92]. We believe that such vulnerabilities are caused by three reasons. First, the EMC is designed to cope with unintentional interference, and its frequency band does not cover the range of effective EMI frequency. The EMC standard mainly considers two types of interference: the conducted interference in the range of $0.15\,\mathrm{MHz} \sim 30\,\mathrm{MHz}$ and the radiated interference in the range of $30\,\mathrm{MHz} \sim 1\,\mathrm{GHz}$ [92]. Yet, the effective EMI signals can be higher than $1\,\mathrm{GHz}$. Second, although low-pass filters are meant to remove all interference signals with a frequency higher than $0.15\,\mathrm{MHz}$, the real filters are not ideal and can let go of high-frequency signals [46]. Last but not least, inverter designs may unintentionally provide backdoors for EMI. For example, ① the LCD screen on the inverter creates a gap of EMC protection and a vulnerable window for EMI; ② the non-ideal printed circuit board (PCB) alignment and device layout bring parasitic capacitance; ③ and the circuit's asymmetrical alignment on the PCB weakens its immunity to common-mode interference; ④ the control algorithms of PV inverters assume the reliability of sensor measurements and lack of consistency checking. Thus, false voltage and current measurements can trick the PV inverter's control algorithms. Currently, most medium-voltage power electronic converters still commonly suffer from parasitic capacitance [57], and current research mainly focuses on predicting and reducing parasitic capacitance [61], [29], [20], [45], [38], but most methods will increase the material and manufacturing cost [57].

To illustrate the impact of the aforementioned vulnerabilities in combination, we design **`ReThink`** (reveal the threat of EMI on inverters) that could produce three types of consequences on PV inverters by emitting carefully crafted EMI, as shown in Fig. 1.

- `DoS`: The PV inverter shuts down completely, causing an instantaneous power reduction of PV generation to the grid or consumers.
- `Damage`: The PV inverter can be physically burned out and has to be repaired or replaced.
- `Damping`: This type of threat causes the output power of PV inverters to be lower than their capability. Long-term continuous `Damping` will reduce the efficiency of the PV generation.

We have validated the consequences of `ReThink` on a PV inverter development kit, 5 off-the-shelf kilowatt-level PV inverters, and a rural-scale microgrid operated in the real world, by transmitting EMI signals at a distance of $100 \sim 150\,\mathrm{cm}$ and emission power within $20\,\mathrm{W}$. Despite the fact that the power capabilities of PV inverters vary from a few kilowatts to 60 kilowatts, the embedded current and voltage sensors operate on a voltage level of $5\,\mathrm{V}$ and are all vulnerable to EMI signals. We have uploaded video demonstrations to the link [2]. To enhance the security of PV inverters, we analyze the underlying causes of the vulnerabilities and propose hardware as well as software countermeasures, including blocking EMI transmissions, detecting measurement manipulation, and repairing control logic vulnerabilities. We hope these can provide guidelines for the design of the PV inverter, e.g., its sensor PCB and control algorithms.

To the best of our knowledge, this is the first systematic work analyzing the impact of EMI on PV inverters and validating on the real-world microgrid. Our work is complementary to existing studies on traditional software or communication-related issues, e.g., software vulnerabilities of inverters or DoS and replay attacks against DC microgrids [90], [7], [52], [85], [65]. The goal of our work is to raise awareness of the security of power electronic devices in the power grids as RES are increasingly being adopted and they represent an emerging CPS threat surface. We imagine that our analysis and conclusions may potentially lay the groundwork for analyzing other types of inverters and power electronic devices with similar sensors and control logic. In summary, our contributions are as follows:

- We present a systematic security analysis of PV inverters and analyze the vulnerabilities of sensors and control algorithms susceptible to EMI signals.
- We illustrate the adversarial `ReThink` scenarios that can shut down, permanently damage, and damp the power output of PV inverters, and we validate the threat on commercial PV inverters and a real-world microgrid.
- We analyze the root causes for the vulnerabilities and propose hardware and software countermeasures.

II. Background and Threat Model

A. Principle of PV Inverter

PV inverters, like many other types of inverters, are the heart of every PV system. To satisfy various design requirements, PV inverters may have subtle differences in their circuit design [33]. After examining 47 inverters from three leading manufacturers [76], [82], [31], we found that 43 inverters employ a standard DC-DC-AC topology, and this predominant architecture is known as a Two-Stage Power Conversion (TSPC) system [16], which is the focus of this paper. Particularly, a PV inverter consists of a power conversion unit, multiple current and voltage sensors, and control algorithms. Since power generation efficiency is one of the most important goals, a PV inverter will track the PV panel's maximum power point (MPP) by sensing and incorporating various control algorithms to convert DC power into AC power. To understand the details, we introduce them below.

1) Power Conversion Unit: A typical TSPC PV inverter contains two parts: the DC-DC stage and the DC-AC stage, as shown in Fig. 2.

DC-DC Stage. The primary function of the DC-DC stage is to increase the voltage level from the PV panel output, e.g., ranging from $30\,\mathrm{V}$ to $60\,\mathrm{V}$, to the one required by power grids, i.e., $325\,\mathrm{V}$ peak for single-phase and $565\,\mathrm{V}$ peak for three-phase.

DC-AC Stage. The DC-AC stage converts the direct current on the DC bus to the AC that can be fed into the grid through the inverter circuit, with the help of two control algorithms, i.e., voltage control loop and current control loop.

[1] Microgrid is a mini version of the grid, where it contains a group of interconnected loads and distributed energy resources and can connect to the grids or operate in an islanding mode [58], [44].

[2] https://tinyurl.com/ReThinkDemoVideos

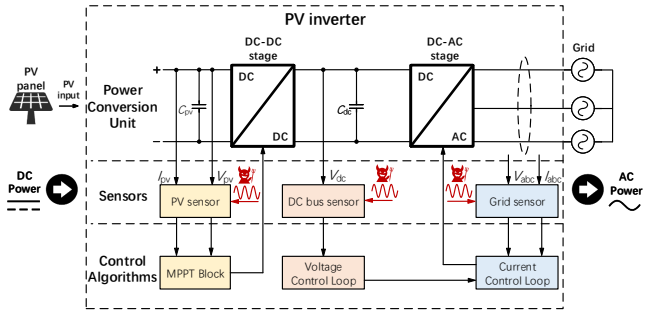


Fig. 2. A typical PV inverter can be modeled as a 3-layer structure: Power conversion unit-Sensor-Control algorithms.

2) Control Algorithm: PV inverter relies on control algorithms to maintain the PV panels or arrays working at their maximum power state and convert DC into AC for integration into the grid. There are three main parts: the maximum power point tracking (MPPT) algorithm, the voltage control loop, and the current control loop.

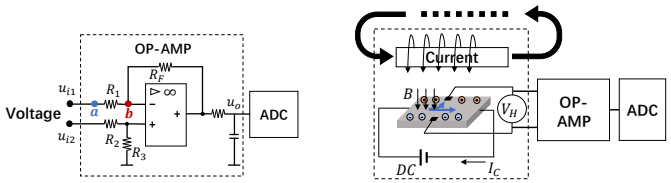
MPPT Algorithm. To maintain the highest energy conversion efficiency in various atmospheres [55], [66], the MPPT operates along a voltage-current (V-I) curve to identify the maximum power point (MPP), where the V-I curve is an inherent characteristic of the PV panel and varies with the irradiance and temperature. The most commonly used MPPT algorithm is the Perturb and Observe (P&O) method, where the basic idea is to try adding a perturbation to the inputs of PV inverters and measure the resulting power [30].

Voltage and Current Control Loop. The role of the voltage control loop is to adjust the DC bus voltage V_{dc} to a reference value. The DC bus capacitor functions as an energy buffer to stabilize the DC bus voltage. If the input power exceeds the output power, the capacitor C_{dc} on the DC bus will continue to be charged, which will lead to an increase in V_{dc} and trigger the voltage control loop to raise the output reference current I_{dref}, as shown in Fig. 22(b). The function of the current control loop is to adjust the output current to match the output power of the PV inverter with its input power. Similar to the voltage control loop, it utilizes a PI controller to adjust the current based on the reference current provided by the voltage control loop. Before entering the PI control, the coordinate system transformations (Clarke & Park) [95] are applied to the measured three-phase voltage and current.

Protection Mechanism of PV Inverter. In the operation of PV inverters, a set of self-protection mechanisms are incorporated to prevent safety issues that may arise from device damage and circuit failure. The mechanisms considered in this paper include DC bus over-voltage protection, as well as AC over and under-voltage protection [80].

• DC bus over-voltage protection. The PV inverter continuously monitors the voltage of the DC bus. If the DC voltage exceeds a predefined threshold several times, the inverter disconnects from the grid and stops power generation.

• AC over and under voltage protection. When the inverter's output voltage is detected to be higher than the threshold range, it will disconnect itself from the grid. If the output voltage drops outside the allowable range of low voltage crossing (20%), the low voltage crossing function will activate, triggering an alarm. If the inverter's output voltage does not recover within a specified time, it will disconnect itself from the grid and stop working.



(a) Non-Hall voltage sensor. (b) Hall current sensor.

Fig. 3. The schematic of voltage and current sensors in the PV inverter [81]. The voltage sensor mainly comprises a differential op-amp circuit; the current sensor comprises a Hall chip and a differential op-amp circuit.

B. Sensors of PV Inverter

As illustrated in Fig. 2, PV inverters rely on embedded sensors to measure voltage and current and feed them back to the control loop.

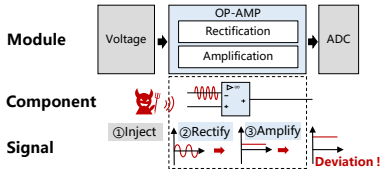
1) Non-Hall Voltage Sensor: Voltage is one of the most important variables in a PV inverter. To detect the voltage in various control loops, voltage sensors convert hundreds of volts into a few volts that the analog-to-digital conversion (ADC) module can handle. Besides, since inverters operate in complex electromagnetic environments and tend to generate common mode noise in the circuits, differential operational amplifiers (op-amp) are often employed to suppress noises [4]. A typical structure of a differential op-amp circuit is shown in Fig. 3(a), and the magnification can be expressed as Equation (1):

$$u_o = \frac{R_3 \cdot (R_1 + R_F)}{R_1 \cdot (R_2 + R_3)} \cdot u_{i2} - \frac{R_F}{R_1} \cdot u_{i1} \tag{1}$$

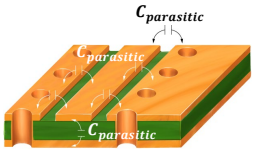
The magnification is determined by the resistors of the op-amp. In practice, resistors R_1 and R_2 usually consist of multiple divider resistors in series, and they step down the high voltage to a low voltage signal within 5 V; *thus, for inverters from a few kilowatts to hundreds of kilowatts, the embedded voltage sensors shall be vulnerable to EMI signals at similar power levels.* The power levels are illustrated in Fig. 19 of Evaluation.

2) Hall Current Sensor: Since the current cannot be directly digitized by ADC modules, inverters typically use a Hall current sensor, which converts the magnetic field generated by the current into DC or AC voltage based on the Hall effect [8].

As shown in Fig. 3(b), the current I generates a magnetic field B, and B is proportional to I according to Ampere's Law. Then the electrons moving on the electrode plate will be subjected to the Lorentz force F_L in B and move to the sides of the electrode plate, and generate an electric field E on the electrode plate. Finally, a balance state will be reached when the electric field force and the Lorentz force are equal, which can be formulated as Equation (2), where d is the width of the electrode plate and q is the electrical charge. Since B is proportional to I and V_H is proportional to B, the Hall sensor's output V_H is proportional to the current I. Finally, Hall current



(a) Transmission process of EMI signals in the voltage sensor.



(b) The parasitic capacitance of sensor's PCB.

Fig. 4. The principle of EMI impact on voltage sensors. The EMI signal is coupled into the sensor circuit, and then rectified, amplified by the op-amp, and ultimately turned into an offset on the output.

sensors use a similar op-amp to suppress the common-mode noise in V_H and output the measurement result.

$$F_L = F_E \Rightarrow B \cdot q \cdot v = q \cdot E = q \cdot \frac{V_H}{d} \tag{2}$$

C. Threat model

We make the following assumptions about the adversary:

Attack Goal. The attacker's goal is to covertly cause the shutdown, power reduction, or even burnout of a PV inverter. Though ambitious attackers may target a group of inverters and try to create potentially escalated impacts such as voltage or frequency fluctuations or even blackouts in a local microgrid, we focus on basic attacks against individual inverters in this paper.

Non-contact Access. We assume the attacker can approach the target inverters within a few meters, but she cannot physically touch or damage them due to safety and stealthiness concerns. Alternatively, the adversary can leave a camouflaged EMI device nearby and control it remotely.

Prior Knowledge. We assume that adversaries could have prior knowledge of the target inverter. Given that many PV inverters are commercial products readily available on the market, the adversary could acquire a PV inverter of the same model and conduct necessary tests beforehand. More favorably, in practice, PV systems in a region often use the same model of PV inverters.

III. Understanding the Impact of EMI on Embedded Sensors of PV Inverters

Sensors provide an entrance for EMI to impact PV inverters. In this section, we explore how EMI affects embedded voltage and current sensors of PV inverters through theoretical analysis and feasibility experiments.

A. Analysis of the EMI Impact on Sensors

The key to exploring the impact of EMI on sensors is to identify the entry points and transmission path of EMI, while considering EMC measures. Given that the voltage sensor contains an op-amp circuit, while the current sensor contains not only an op-amp but also a Hall element, we analyze them separately.

1) Impact of EMI on Voltage Sensors: The sensor's PCB usually carries parasitic capacitance and is susceptible to electromagnetic interference in the environment. Besides, the op-amp circuit will further rectify and amplify the coupled signals. The transmission process can be illustrated in Fig. 4(a), and there are four steps:

• **EMI signal injection.** Process ① in Fig. 4(a) is EMI injection. Electromagnetic fields around the sensor can be injected into sensor circuits (e.g., input nodes) via electromagnetic coupling. Generally, according to the EMI transmission paths, EMI coupling methods can be divided into conductive coupling, inductive coupling, capacitive coupling, and radiative coupling (also called radio frequency interference, RFI) [3], [75]. Among them, radiative coupling refers to the far-field coupling of higher-frequency signals in the microwave frequency range, which can be transmitted over longer distances. Notably, the conductors (e.g., copper wires and component pins) and the insulator (e.g., PCB substrate) on the sensor's PCB will form parasitic capacitance, as shown in Fig. 4(b). These parasitic capacitances are susceptible to the aforementioned high-frequency electric fields, which can introduce interfering signals. Thus, high-frequency EMI signals can be effectively coupled into the sensor circuits via radiative coupling.

• **Nonlinear rectification effect.** The amplifier can rectify the high-frequency AC signal at the input and generate a DC bias at the output. The main reason is that the bipolar junction transistor (BJT) in the op-amp chip contains p-n junction diodes, which are efficient rectifiers due to their nonlinear current-voltage characteristics, especially in low-power op-amps [15]. When a high-frequency signal $v(t) = V_X cos(2\pi f_X t)$ is injected into the base-emitter junction of an op-amp BJT-based input stage, the output will generate an AC term $\Delta i_C(AC)$ at twice the input frequency and a DC term $\Delta i_C(DC)$ [15], which can be described by Equation (3):

$$\Delta i_C(DC) = (\frac{V_X}{V_T})^2 \cdot \frac{I_C}{4} \tag{3}$$

• **Asymmetric differential effect.** The asymmetric design of the op-amp circuit on the PCB allows the output bias of the op-amp to be **positive** or **negative**. As shown in Fig. 5, an op-amp channel consists of a differential amplification input stage, an intermediate amplification stage, and a push-pull output stage. The transfer relationship of the differential amplification input stage can be expressed as:

$$V_{o1} - V_{o2} = A_d(V_{i1} - V_{i2}) + A_c(V_{i1} + V_{i2}) \approx A_d(V_{i1} - V_{i2})$$

where A_d is the differential-mode gain and A_c is the common-mode gain.

The asymmetric design of the input stage's wires results in different frequencies of EMI coupling. Consequently, the EMI signals coupled into V_{i1} and V_{i2} will differ, ultimately producing a positive or negative output. This outcome depends on whether the coupled signal is stronger at V_{i1} and V_{i2}. To demonstrate, we build the circuit model of the OPA2171 chip in Simulink, as shown in Fig. 28 in Appendix C. We inject the sinusoidal signal in Fig. 6(a) to V_{i1}, V_{i2} or both, and we find that the output can be positive, negative, or 0 respectively, as shown in Fig. 6(b), Fig. 6(c) and Fig. 6(d). Therefore, the

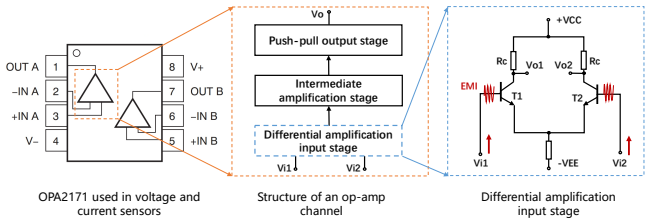
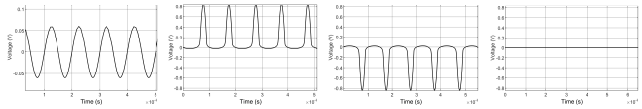


Fig. 5. The structure of the OPA2171 used in voltage and current sensors.



(a) Input signal. (b) Output (inject from V_{i1}). (c) Output (inject from V_{i2}). (d) Output (both inject).

Fig. 6. Simulation of EMI injection on different inputs of the op-amp chip.

attacker can tamper with the sensor's output to a larger or smaller value by adjusting the frequency of the EMI signal.

• **Amplification effect.** Amplification is the fundamental function of op-amp. Signal inputs will be amplified according to the set gain; however, EMI signals can enter into various nodes via radiative coupling. As shown in Fig. 3(a), when the EMI signal is injected into the node b, it can be considered that $R_1 = R_2 = 0$. Then, according to Equation (1), the gain will be abnormally large. In other words, even if injecting a millivolt signal at node b, it can be amplified to a few volts in process ③ of Fig. 4(a).

In conclusion, electromagnetic coupling enables the injection of EMI, the nonlinear rectification converts alternative interference into positive bias, the asymmetric differential effect allows the bias to be positive or negative, and the amplification effect amplifies the injected EMI signals.

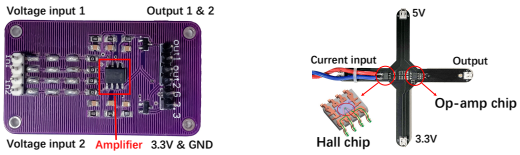
2) Impact of EMI on Current Sensors: Unlike the voltage sensor, the current sensor includes not only an op-amp circuit but also a Hall element, which may serve as a new entrance for EMI. Thus, we mainly analyze how EMI can enter the sensor circuit through the Hall chip.

We have already described that Hall current sensors measure current indirectly by measuring the magnetic field generated by the current, and the measurement relies on the balance of the Lorentz force and electric field force on the electrons, as shown in Equation (2). Thus, an additional magnetic or electric field around the Hall chip will impact the current measurement, either directly or indirectly. Now we discuss them separately:

• **Impact of magnetic field on Hall sensor.** We assume the measured current generates a magnetic field B in the Hall element. Since the output V_H is proportional to B, we quantify this as Equation (4). If EMI generates a magnetic field B_A nearby, B_A will be superimposed on B. Therefore, the output of the Hall element may be directly manipulated by the EMI signal, and this relation can described as Equation (5), and the output V_H of the Hall element will be changed by $k \cdot B_A$.

$$V_H = k \cdot B \tag{4}$$

$$V_H^* = k \cdot (B + B_A) = V_H + k \cdot B_A \tag{5}$$



(a) Voltage sensor. (b) Current sensor.

Fig. 7. The voltage and current sensors' PCB we designed for the initial feasibility test.

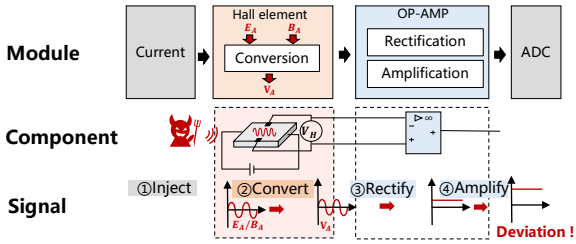


Fig. 8. The principle of EMI impact on Hall current sensors. The EMI signal is injected into the Hall chip and generates a noise V_H. Then the noise will be rectified, amplified by the op-amp, and result in a deviation on the output.

• **Impact of electric field on Hall sensor.** According to Equation (2), we have

$$V_H = d \cdot E \tag{6}$$

If an additional electric field E_A exists near the Hall chip, at this point we have

$$V_H^* = d \cdot (E + E_A) = V_H + d \cdot E_A \tag{7}$$

Thus, the output V_H of the Hall chip will be changed by $d \cdot E_A$, where d is the width of the electrode plate.

Then, the affected output V_H^* will continue to be rectified and amplified by the op-amp and finally generate a bias on the measurement, as shown in ③ and ④ in Fig. 8.

It is worth noting that since the output V_H of the Hall chip is fed into the positive input of the op-amp, the EMI injected into the Hall chip will theoretically result in a positive bias in the current measurement. However, the EMI can also affect the op-amp of the current sensor, which will cause positive or negative bias.

B. Experimental Verification

To verify the previous analysis, we conducted feasibility tests to explore the capability of EMI to impact sensors of PV inverters.

1) Can EMI Impact Voltage and Current Sensors: We conduct an EMI frequency sweep test on voltage and current sensors. The experiment setup is shown in Fig. 9, and the test steps are:

① In the feasibility verification stage, we built the PCBs of the voltage and current sensors according to the schematic of the C2000 PV inverter from Texas Instruments (TI) that we have in hand [81], as shown in Fig. 7(a) and Fig. 7(b).

② We use a DC power source RIGOL DP711 [62] to generate a 30 V voltage and $0 \sim 5$ A current to be measured. Then, we use the Arduino UNO to read the voltage every

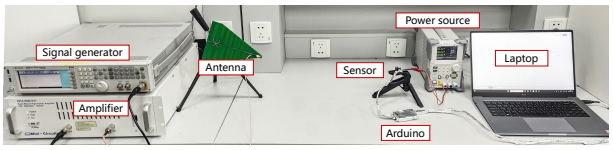
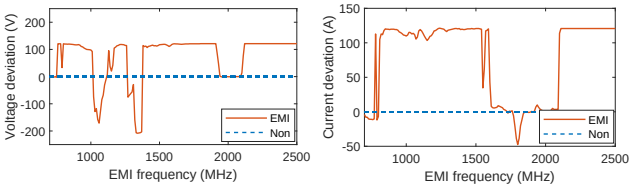


Fig. 9. Setup of feasibility test on sensors.



(a) Voltage sensor. (b) Current sensor.

Fig. 10. The result of the EMI frequency test on the voltage and current sensors. The EMI power and distance are set to 10 W and 50 cm.

10 ms and send the data to the PC through the serial port. The Arduino is wrapped in EM shielding material to prevent EMI. All components are readily available on the market.

③ Subsequently, we use EXG vector signal generator [77] to generate a 700 MHz $\sim$ 2.5 GHz signal, use amplifier HPA-50W-63+ [51] to amplify it to 10 W, and emit it with a 5G directional antenna [72] with $+14$ dBi at a distance of 50 cm.

We record the deviation of the measurements in Fig. 10. For the voltage sensor, the measured voltage can be decreased by 200 V and increased by 120 V at most. For the current sensor, the measured current can be increased by up to 320 A and decreased by up to 30 A. The result demonstrates that EMI can effectively affect the voltage and current sensor's outputs. Notably, in the test of the Hall current sensor, the deviation of the measurement is predominantly positive. This verifies our previous analysis of the impact of EMI on current sensors.

To further verify that the EMI can impact the Hall chip directly, we conducted a small test: We measured the output V_H of the Hall chip using RF wines to avoid wire coupling, with the sample rate of 10 GHz, and compare the effect of EMI on V_H. The result is shown in Fig. 29 in Appendix C. It shows that EMI can directly impact the Hall chip by inducing a 0.2 V bias and a 0.5 V oscillation on the output V_H of the Hall element.

2) Whether the Impact is Controllable: To explore the EMI manipulation capability on sensors, we tested two kinds of EMI signal modulation methods:

① Frequency modulation (FM). Fig. 10(a) and Fig. 10(b) reveal that sensors have different "sensitivity" to EMI signals of various frequencies. It appears that adjusting the signal frequency may manipulate the target sensor's output. However, we can also find that the sensor's output varies significantly as the frequency changes. Therefore, achieving precise control of sensor values with FM proves challenging.

② Amplitude modulation (AM). Another signal modulation method is AM, as described in Equation (8), where $s_m(t)$ is the modulation signal, A_c and f_c are the amplitude and frequency

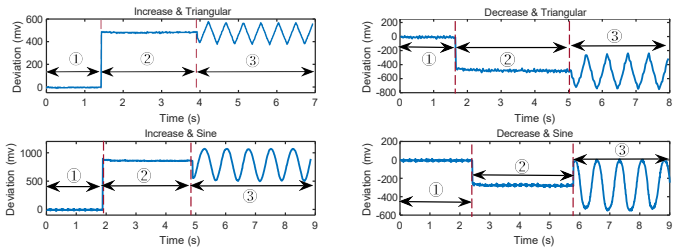


Fig. 11. The experiment result of manipulation with a single-frequency signal and an AM signal on the sensor. ①:Without EMI; ②:Single-frequency EMI; ③:AM-modulated EMI.

of the carrier signal $s_c(t)$.

$$s_{AM}(t) = A_c[1 + s_m(t)]cos2\pi f_c t \tag{8}$$

Since the offset of the sensor's output is proportional to the amplitude of the EMI signal, we first select a carrier signal $s_c(t)$ that can impact the sensor's output, then set $s_m(t)$ to the "desired" curve, which is also the envelope of $s_{AM}(t)$.

In this scenario, assuming that one wants the measured voltage to first increase or decrease and then change as the triangular or sine wave, we conducted an experiment using AM. The result is highly "favorable" for an adversary, as depicted in Fig. 11. Although the real voltage or current remains constant, the measured values change precisely by the $s_m(t)$, such as triangular and sine waves.

3) Verification of the Universality and Extensibility: Commercial PV inverters usually contain multiple types of sensors. To analyze the universality of the threat, we propose two questions: ① What is the impact of EMI on different Hall sensors? ② If there are multiple sensors, can EMI only impact a single target sensor or control multiple target sensors simultaneously?

Universality. To answer the first question, we evaluate the impact of EMI on 7 different Hall sensors, including 4 analog sensors and 3 digital sensors. Hall digital sensors include a speed sensor, a north pole sensor, and a water flow sensor. The result is presented in Table I. We can find that both wired and wireless Hall current sensors are susceptible to EMI, and wireless Hall current sensors exhibit a higher degree of susceptibility. Hall sensors with digital outputs, like speed sensors, may experience bit-flipping under EMI.

Extensibility. Since EMI signals of different frequencies can be injected into different nodes of the victim circuit, we can establish a frequency sweep model for each sensor and implement the following: ① "one-to-one" manipulation: select a frequency that exclusively affects the target sensor without impacting others; ② "many-to-many" manipulation: when manipulating several sensors simultaneously, owing to the superposition of EMI signals, we can employ different channels to emit EMI signals of various frequencies. *This feature also highlights one of the advantages of EMI over constant magnetic field attacks in Hallspoofing [6]: higher extensibility in signal design through signal multiplexing.*

TABLE I. RESULT OF EMI IMPACT ON 7 HALL SENSORS

Sensor type	Sensor model	Output type	Measure-ment span	Test parameters		Output				
				Freq.(MHz)[3] (Pos. /Neg.)[3]	Pow.(W)[3]	Original value	Pos. dev.[1,3]	Pos. dev. rate	Neg. dev.[1,3]	Neg. dev. rate
Current	WCS1800 (Wire)	Analog	0∼30A	685/1030	10	5 A	15.7 A	+214.00%	-6.1 A	-222.00%
Current	WCS1800 (Wireless)	Analog	0∼35 A	1000/876	10	5 A	31.5 A	+530.00%	-7.6 A	-252.00%
Current	ACS712 (20 A)	Analog	0∼20 A	779/1223	10	5 A	13.2 A	+164.00%	-13.2 A	-364.00%
Current	ACS712 (5 A)	Analog	0∼5 A	627/1212	10	2.5 A	5.1 A	+104.00%	-7.75 A	-410.00%
Speed	3144	Digital	0/1	677	10	0/1	bit-flap[2]	+100.00%	bit-flap	-100.00%
North pole	3144	Digital	0/1	724	10	0/1	bit-flap	+100.00%	bit-flap	-100.00%
Water flow	YF-S401	Digital	0/1	1322	10	0/1	bit-flap	+100.00%	bit-flap	-100.00%

[1] For each Hall current sensor, we repeat each experiment 10 times and calculate the average deviation.
[2] For each Hall digital sensor, we only record whether the output experiences a bit-flip.
[3] "Freq." means frequency; "pos." and "neg." means positive and negative deviation; "dev." means deviation.

IV. UNDERSTANDING THE IMPACT OF SENSOR SPOOFING ON PV INVERTERS

Here, we analyze how the spoofing of sensors affects the operation of PV inverters. We build the PV inverter circuit model and implement the control algorithms outlined in Section II using Simulink.

A. Impact of DC Bus Voltage Sensor

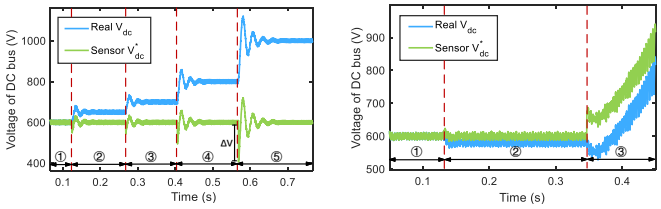
Deceiving the DC bus sensor will directly affect the DC bus voltage control loop. The function of the voltage control loop is to maintain the DC bus voltage V_{dc} as its reference value V_{dcref} set by the manufacturer. When an EMI signal introduces a deviation of V_a on the measured bus voltage, it will lead to Equation (9):

$$V_{dc}^{*} := V_{dc} + V_a \tag{9}$$

Then the controller will adjust V_{dc}^{*} to be equal to V_{dcref}, and the real DC bus voltage will become $V_{dcref} - V_a$ under control. This will cause the following damages.

1) Breakdown of DC Bus Capacitor ($V_a < 0$): If the EMI signal introduces a negative V_a to the measured V_{dc}, the real DC bus voltage will increase and the aging of the DC bus capacitor C_{dc} will accelerate. The capacitor will break down when the voltage exceeds the rated voltage of the C_{dc}. While the inverter incorporates over-voltage and under-voltage protection mechanisms, the vulnerability could persist, potentially leading to physical damage. This risk emerges when the adversary intentionally avoids injecting V_a with a substantial magnitude in a single instance. This is attributed to continuously manipulating sensor values to appear within their normal range while the real DC bus voltage is spoofed. For the adversary, he may want to ensure that, during the injection of the EMI signal, the sensor value does not trigger the under-voltage protection mechanism, allowing the EMI to circumvent the protective measures. Afterward, the inverter loses its ability to operate correctly due to the deficiency in the C_{dc}'s capacity to balance the input and output power.

The simulation results are given in Fig. 12(a). It can be observed that the real DC bus voltage is increased by 50 V, 100 V, 200 V and 300 V after sensor manipulation. Looking at Fig. 12(a) for the case of $V_a = -300$ V, the transient voltage offset ΔV will trigger the protection instantly and shut down the inverter.



(a) $V_a < 0$. (b) $V_a > 0$.

Fig. 12. The simulation of the DC bus voltage manipulation. We add a fake V_a on the measured DC bus voltage and record the real DC bus voltage under control. For $V_a < 0$, ①: $V_a = 0V$, ②: $V_a = -50V$, ③: $V_a = -100V$, ④$V_a = -200V$, ⑤$V_a = -300V$; for $V_a > 0$, ①: $V_a = 0V$, ②: $V_a = 20V$, ③: $V_a = 100V$.

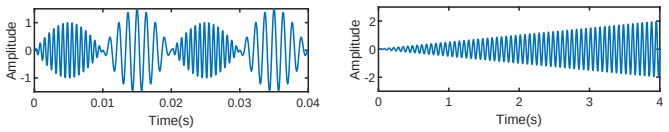
2) DC Bus Under-voltage ($V_a > 0$): Similarly, an adversary can decrease the real DC bus voltage by injecting a positive V_a into the voltage measurement. If the real DC bus voltage drops below the lower threshold, the output AC voltage will be lower than the grid voltage. In that case, the current will be reversed, and the power will flow back from the grid to the inverter, and the protection mechanisms will be triggered to shut down the inverter. This process is shown in Fig. 12(b) when $V_a = 100$ V.

Hence, in summary, the impact of sensor spoofing on the DC bus voltage can be articulated as follows:

Impact 1: `DoS`. The `DoS` stops the PV inverter's normal operation. The key of `DoS` is to trigger the self-protection mechanism of PV inverters. As previously analyzed, there exist two methods to induce `DoS`. Here, we illustrate the process by taking the example of injecting a positive deviation ($V_a > 0$) on the DC bus voltage sensor. To achieve this objective, the adversary could design the EMI by the following steps:

To begin, it is imperative to carefully select the frequency f_{c+} of the EMI signal through preliminary frequency testing. This choice can potentially augment the measured V_{dc}. Given that PV inverters of similar application levels, such as residential PV inverters ranging from 1 kW to 60 kW, typically share similar PCB dimensions, the frequencies susceptible to EMI do not show substantial variations. Drawing from our empirical observations, f_{c+} commonly falls within the range of 700 MHz to 1500 MHz. Subsequently, as the adversary approaches the PV inverter, it becomes necessary to transmit the EMI signal at the designated frequency f_{c+} for a brief duration, typically spanning a few seconds.

Impact 2: `Damage`. `Damage` can potentially result in the



(a) EMI signal for DoS on AC side. (b) EMI signal for Damage.

Fig. 13. Design of EMI signals $s(t)$ of DoS and Damage.

permanent breakdown of the DC bus capacitor and inflict harm upon the PV inverter. To effectuate Damage, an adversary must elevate the real V_{dc} by introducing a negative V_a into the measured V_{dc} while circumventing the activation of the self-protection mechanism.

First, the adversary needs to find the frequency f_{c-} that can efficiently decrease the measurement of V_{dc} and generate the carrier signal $s_c(t)$. Since the victim system takes time to reach the stability of V_{dc} after each manipulation, the adversary can design $s_m(t)$ as, Equation (10), where k and s_0 are the scale factor and initial value of $s_m(t)$. Generally, the smaller k is, the easier it is to avoid triggering the self-protection mechanism, but it takes a longer time. Finally, the adversary obtains $s(t)$ by AM, as shown in Fig. 13(b).

$$s_m(t) = kt + s_0, \ k > 0, \ s_0 \geq 0 \tag{10}$$

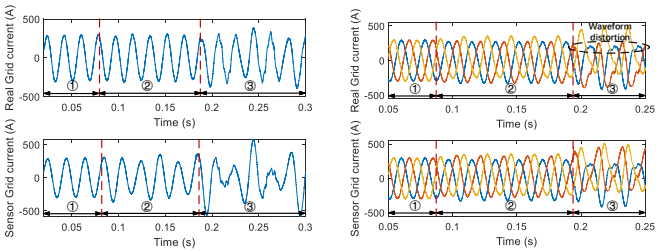
To avoid triggering the protection mechanism, for the TI C2000 PV inverter [80], the target V_{dc} is 385 V, and the safety range is 220 V $\sim$ 395 V. It indicates that the adversary needs to allow time for the controller to adjust V_{dc} within this range after each manipulation.

B. Impact of Grid Voltage and Current Sensors

The measured grid voltage and current serve as feedback for the current control loop. Manipulations on these sensors have different effects on single-phase and three-phase PV inverters. The three-phase inverter supplies a three-phase AC power output that the phases are 120° between each other, commonly used in industrial and commercial settings. The single-phase inverter outputs one-phase AC power, typically employed in residential PV generations.

1) Single-phase PV Inverter: We take the manipulation of grid current as an instance. If the injected deviation I_a is constant, there will be a "transient effect" on the real grid current. This is similar to the case in which the inverter suffers from sudden grid current changes while the control loops manage to restore the current. To illustrate, let I_a be constant and positive, then the controller will decrease the current, and the inverter's output power will decrease. However, when the output power becomes less than the input power, the DC bus capacitor will charge, leading to $V_{dc} > V_{dcref}$, and the current reference will increase. In this regard, the reference will rise again to catch up with the manipulated current.

To note, if the injected deviation I_a is time-varying, like a sinusoidal signal, the PV inverter will not enter into a steady state. The simulation result is shown in Fig. 14(a). The larger the magnitude of the injected deviation I_a, the higher the degree of oscillation in the grid current. When the oscillation reaches a certain level, the grid current and voltage will exceed the threshold and trigger the protection mechanism, and the inverter will shut down.



(a) Single-phase PV inverter. ①:$I_a = 0A$, ②:$I_a = 50\sin\omega tA$, ③:$I_a = 200\sin\omega tA$.

(b) Three-phase PV inverter. ①:$I_a = 0A$, ②:$I_a = 50A$, ③:$I_a = 200A$.

Fig. 14. The simulations of grid current sensors spoofing. It gives the simulated waveform of the real current value and the sensor output value when the single-phase and three-phase grid current measurement is manipulated.

2) Three-phase PV Inverter: As mentioned in the background, the three-phase voltage and current output of the PV inverter need to be transformed into the coordinate system through the Clark transformation and Park transformation before entering the control loop. In fact, due to this coordinate system transformation, a constant injected deviation into the three-phase voltage and current measurements could not affect the inverter's output. This is because it will be filtered out by the Clark transformation matrix. *Thus the Hallspoofing attacks in [6] may fail in such scenario.*

Therefore, the impact of grid voltage and current sensor manipulation in the three-phase PV inverter will only manifest when the injections are "unequal". As illustrated in Fig. 14(b), compared to the single-phase inverter that needs to inject a time-varying I_a, the three-phase inverter only needs to inject a constant I_a into one phase but not other phases to achieve a similar impact (inverter shutting down). The coordinate system is time-varying, making the component on each axis of the time-invariant signal also time-varying. For simulations of measurement manipulation on grid voltages, we refer to Appendix B1. We now summarize the impact of grid voltage and current sensor spoofing on PV inverters:

Impact: DoS. For DoS impact on the grid AC side, the primary adversarial strategy involves inducing oscillations in the AC voltage or current. Taking the AC current as an example, the adversary needs to inject a time-varying signal $I_a(t)$ on the measured AC current. We select $I_a(t)$ as a sine wave with the same frequency as the AC, which is not the only option.

$$I_a(t) = A_a \cdot sin(2\pi f_{AC} t) \tag{11}$$

where f_{AC} is the AC frequency, and A_a is the amplitude of $I_a(t)$. Since the grid imposes strict limitations on input voltage and current, an $I_a(t)$ with a few amps is enough to achieve the impact of DoS.

First, the adversary needs to find the frequency f_{c+} and f_{c-} that can increase and decrease the measured AC current. Then he may design the modulation signal $s_m(t)$ as:

$$s_m(t) = sin(2\pi f_{AC} t) \tag{12}$$

Finally, get the EMI signal $s(t)$, as shown in Fig. 13(a),

$$s(t) = \begin{cases} A_+(1+s_m(t))cos2\pi f_{c+}, s_m(t) > 0, \\ A_-(1+s_m(t))cos2\pi f_{c-}, s_m(t) \leq 0 \end{cases} \quad (13)$$

The adversary only needs to continuously transmit the signal for a few seconds when passing by the target inverter.

C. Impact of PV Voltage and Current Sensors

The PV voltage and current sensors are used for the MPPT algorithm and the DC-DC stage. Since the MPPT algorithm regulates the input power of the inverter by controlling the input voltage, manipulating V_{pv} and I_{pv} can impact the output power of the PV inverter.

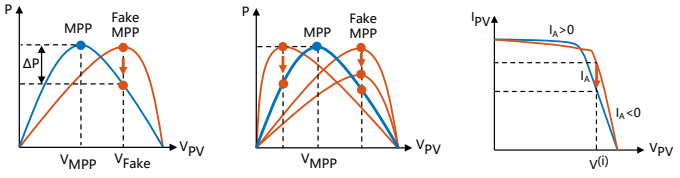
Injecting a constant offset ΔV on the PV voltage sensor or ΔI on the PV current sensor (Fig. 27(a) in Appendix B) only shifts the V-I curve without changing its "shape". Thus, the MPPT algorithm will still find the correct MPP with false measured V_{pv} or I_{pv} by the P&O algorithm.

However, if the adversary can design a fake V-I curve with a different shape from the original one, the MPPT algorithm will be misled into finding the fake MPP, resulting in decreased power. To inject a fake V-I curve, the adversary needs to make the spoofed points (V_{pv}, I_{pv}) move on a fixed but false curve by manipulating the measured I_{pv} or V_{pv}, as shown in Fig. 27(c) in Appendix B. We will specify this method in the following.

Impact: `Damping`. `Damping` will adversely impact the efficiency and reduce the output power of PV inverters. The primary objective of the `Damping` is to deceive the MPPT algorithm, preventing it from accurately identifying the MPP. Two distinct EMI design strategies for achieving this objective exist, categorized as "spoofing" and "interference". The "spoofing"-based method quantitatively diminishes the power output of the target PV inverter but necessitates the utilization of feedback information, namely V_{pv} and I_{pv} values from the internal sensors of the PV inverter. Conversely, the "interference"-based method can relatively reduce the power of the PV inverter without requiring any feedback information.

For the `Damping` based on "interference": Since the MPPT finds the MPP by P&Q method that relies on stable V_{pv} and I_{pv}, the adversary could tamper with V_{pv} or I_{pv} to interfere the MPPT. The EMI threat can be designed akin to the `DoS` scenario to disrupt the measurement of V_{pv} or I_{pv}, thereby impeding the MPPT algorithm from achieving maximum power. According to our experiment on the TI C2000 PV inverter, the injected V_a should be between -5 V and $+5$ V to avoid triggering `DoS` impact instead; this threshold can be obtained by pre-test.

For the `Damping` based on "spoofing": First, an adversary needs to acquire the V-I or V-P characteristic curve $f(V, I)$ from the user's manual of the PV panel. Without this information, the attacker needs to buy the same model of PV panel and measure the voltage and current under different insolation and temperatures to plot the V-I curve. Then, the adversary needs to design a fake V-I curve $f^*(V, I)$, and the MPPT algorithm will reach the false MPP on the fake V-I curve. The real power will be reduced by ΔP, as shown in Fig. 15(a). There are diverse fake V-P curves, as indicated in Fig. 15(b). The challenge lies in making the point (V_{pv}, I_{pv}) move on the fake V-I curve



(a) V-P curve. (b) Diversity of the curve. (c) V-I curve.

Fig. 15. False V-I curve design of `Damping` based on the "spoofing" method.

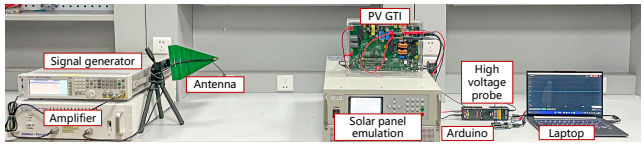


Fig. 16. Experiment setup of evaluation on PV inverters.

$f^*(V, I)$ at any time. To achieve this, one feasible solution is to adjust I_{pv} according to V_{pv}, as illustrated in Fig. 15(c), and the steps can be summarized as follows:

First, the adversary needs to design a fake V-I curve $f^*(V, I)$. When approaching the victim PV inverter, the adversary reads the V_{pv} and I_{pv} via the pre-installed sensors in the inverter as the feedback information and adjusts I_{pv} to the fake V-I curve by adjusting the EMI power. The pseudo-code is illustrated in Algorithm 1.

Algorithm 1 `Damping` based on "spoofing"

Input: Measured PV voltage V_{pv}, measured PV current I_{pv}
Output: EMI power P

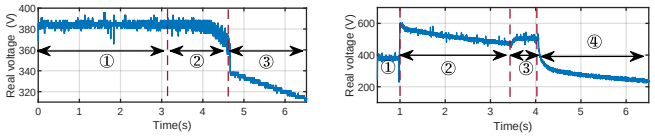
```
while 1 do
    Read V_pv
    Read I_pv
    Get expected I*_pv according to V_pv and fake V-I curve
    if I_pv < I*_pv then
        Adjust EMI power P_A to increase I_pv
    else
        Adjust EMI power P_A to decrease I_pv
    end if
    Wait inverter to update V_pv and I_pv
end while
```

V. Threat Evaluation

In this section, we first evaluate the threat of `ReThink` on PV inverters, and then test on a rural-scale microgrid operated in a real world to explore the impact of `ReThink` on the grid. To our knowledge, this is the first work validating EMI threat on the real-world microgrid. *To ensure the safety and legality of the research, we conducted all indoor experiments in an electromagnetic shielding room, and we contacted the manufacturer and local distribution grid operator about the testing details to avoid ethical problems.*

A. Evaluation on PV Inverters

1) Experiment Setup: As shown in Fig. 16, the experimental setup comprises victim and adversary devices. The victim devices are off-the-shelf PV inverters, and adversary devices are used to emit EMI signals.



(a) Result of DoS. ①: Before EMI, ②: EMI begins, ③: After EMI.

(b) Result of Damage. ①: Before EMI, ②: EMI begins, ③: Burning out, ④: After EMI.

Fig. 17. The experiment results of DoS and Damage.

Victim Devices. To verify the universality of the threat, we select a TI C2000 inverter development kit [80] and 5 commercial PV inverters [26] [42] [32] [27] from well-selling manufacturers, as shown in Fig. 30 in Appendix C. The inverters [80] [26] [42] [32] are tested under laboratory conditions, and 2 models of inverters designed by GoodWe [27] are tested in a real-world microgrid.

Compared with commercial inverters, the TI inverter development kit has the following features: ① lower power and higher safety; ② most of the process variables can be read from the upper computer; ③ open-source control programs. In comparison, commercial PV inverters ① have better EMC countermeasures (such as special enclosures and internal filtering circuits); ② operate at higher power levels (several kWs), posing risks for conducting Damage experiments; thus we evaluate all three impacts of ReThink on the C2000 solar micro inverter and evaluate DoS and Damping on 5 commercial inverters.

Test-bed devices. To support the victim inverter's operation, we use a programmable solar panel emulator TEWERD TPV1000 [78] to emulate solar panels and a RIGOL RP1025D high voltage differential probe [63] to acquire the real voltage.

Adversary devices. The adversary devices are the same as those introduced in Section III. They are used to generate, amplify, and emit EMI signals. *To prevent the adversary devices from causing conducted interference to the victim's PV inverter through the public grid, we added a fourth-order low-pass filter between the adversary devices and the grid to eliminate conducted interference.*

2) Evaluation of DoS: We have introduced in Section IV that DoS impact can be induced in two ways:

DoS on the DC side. Taking the TI C2000 inverter as an instance, we use a signal generator and RF amplifier to generate a signal with the frequency of 735 MHz and the power of 10 W, and emit it with the antenna. As the measured V_{dc} has been tampered with, we use the high-voltage probe to acquire the real V_{dc}, as shown in Fig. 17(a).

As we can see, before DoS, the PV inverter works correctly, and V_{dc} remains stable at around 385 V. When EMI is initiated, we gradually increase the measured V_{dc} to "deceive" the controller. As we presupposed, the controller reduces the real V_{dc}, and finally, the inverter shuts down at 4.5 s due to current back-flow caused by under-voltage. The process can be seen in the video [2].

DoS on the AC side. We first select the frequencies 1000 MHz and 1080 MHz that can respectively increase and decrease the measured AC voltage V_{abc} through a frequency sweep. Then we generate EMI signal $s(t)$ by AM as described in Section IV. The frequency of $s_m(t)$ is set to be the grid frequency of 50 Hz, and the total power is set to 10 W, although the selection of $s_m(t)$ is not unique. We can see that the "Over-Grid Voltage" alarm is triggered when the measured V_{abc} increases to 240 V, and the "Under-Grid Voltage" alarm is triggered when the measured V_{abc} is lower than 200 V [2].

The evaluation of DoS on commercial inverters are similar, and the result is shown in Table II. As we can see, ① the DoS on commercial inverters need more EMI power, which is consistent with our observation: commercial inverters have better EMC countermeasures; ② the impact of DoS on the AC side is more challenging to achieve, compared with DoS on the DC side.

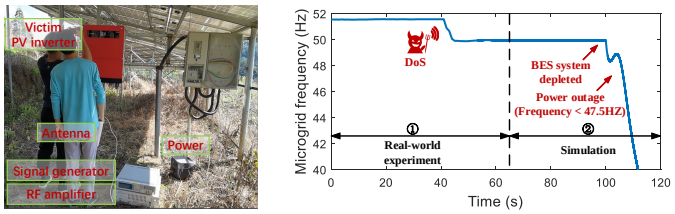
3) Evaluation of Damage: Damage can cause physical damages to the PV inverter by increasing the real V_{dc}. Through pre-test, we find that the 1350 MHz EMI signal can reduce the measured V_{dc}. We adjust the total power from 5 W to 20 W and emit it with an antenna. We use the high-voltage probe to measure the real V_{dc}.

The result is depicted in Fig. 17(b). In phase ①, the PV inverter works correctly, and V_{dc} remains stable at the target value of around 385 V. In phase ②, we emit EMI signal $s(t)$ and the controller increases the real V_{dc} beyond 500 V. At around 3.5 s, the DC capacitor gets a dielectric breakdown and burns out after a few seconds. However, the PV inverter is "unconscious", and V_{dc} continues to rise from 3.5 s to 4 s. To prevent any danger, we terminate the test and cut off the power supply at 4 s and the voltage V_{dc} decreases to 0, as shown in video [2].

4) Evaluation of Damping: Based on the analysis in Section IV, if the adversary is assumed to have feedback information such as the input voltage V_{pv} and current I_{pv}, he can pose a greater threat by decreasing the maximum power quantitatively. Here we focus on the scenario where no feedback information is available and evaluate the Damping impact based on the "interference" method.

For the C2000 PV inverter, we set the input power of the inverter to 80 W, and then transmit a 1350 MHz EMI signal and alternately switch it on and off. We find that the inverter's power is reduced to 30 W and cannot be automatically adjusted to 80 W during the Damping [2]. This indicates that Damping can interfere with the MPPT algorithm and reduce the inverter's power by 62.5%.

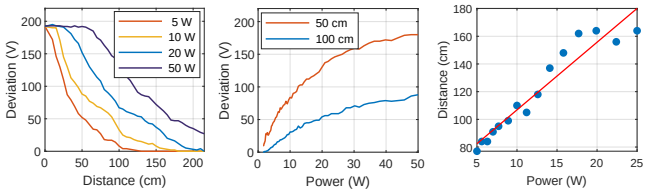
For commercial inverters, we set the same V-I curve with a maximum power point of 2000 W in the PV emulator. In the usual case, they can work stably at 1980 W, 1995 W and 1960 W. Then, we conduct the Damping with a total power of 20 W and record the power according to the PV emulator. As shown in Table II, the power of Ginlong, Kstar, and Huawei PV inverters can be reduced by 150 W, 105 W and 110 W at most, respectively. Besides, we implemented the same experiment on GoodWe inverter [27] under a real-world microgrid, and its power is reduced from 35.6 kW to 2 kW. The difference in reducible power is mainly caused by the perturbation resistance of different MPPT algorithms and the difference between the PV emulator in the laboratory and the real PV panel in the real-world microgrid.



(a) Experiment setup in the real-world microgrid.

(b) Impact of DoS on microgrid frequency.

Fig. 18. The impact of DoS on a real-world PV microgrid's frequency. stage① real-world experiment, stage② simulation.



(a) Distance→sensor. (b) Power→sensor. (c) Dis.& Pow.→ DoS.

Fig. 19. The influence of distance and power to manipulate inverter sensors and DoS a commercial inverter. The nonmonotonicity in (c) is mainly because the power will affect the electromagnetic field distribution of the antenna, which is not linear.

Compared with DoS, Damping can be more insidious in some sense. On the one hand, it can be utilized to affect the power conversion efficiency of PV generation in the long term; on the other hand, it can launch in an on/off pattern (i.e., switching attacks) to affect the PV microgrid, as discussed in Section VI-C.

B. Evaluation on PV Microgrid

To demonstrate the threat of EMI to the real-world grid, we collaborate with the local distribution grid operator and conduct the DoS and Damping experiments on a real-world microgrid, ensuring safety and minimal disruption to residents' daily lives.

The topology of the microgrid is shown in Fig. 25 in Appendix C. The microgrid has a capacity of 400 kVA, and the maximum generated power of PV is 323 kW. The total load is usually between 12 kW and 40 kW. To ensure a continuous and stable power supply, the microgrid is designed with a 150 kWh battery energy storage (BES) system. It can operate in grid-connected or islanding mode, serving a discrete footprint of a remote mountain village. The PV microgrid contains 2 types of 5 PV inverters designed by GooDWe with the power of 50 kW and 60 kW.

In the islanding mode of the microgrid, we first evaluated DoS and Damping on each inverter. Then we perform DoS on all 5 PV inverters and lasts for around 1 min. We investigated the impact of the DoS on the islanding mode microgrid and recorded the frequency of the microgrid in Fig. 18.

It can be observed that there is a decrease in the microgrid frequency by 1.5 Hz. This shift is caused by the deficiency of PV generation at the point, prompting the BES system from the P/Q control [17] to V/f control [9]. The P/Q mode controls the output power of the PV-BES system, while the V/f mode controls the output voltage/frequency by the BES output. This indicates that the microgrid is now solely powered by the BES system, and the battery energy is continuously depleting. Notably, such a condition, mainly when the battery is low on energy, may cause more severe consequences.

However, we are not permitted to conduct the experiments under conditions of extreme low power storage that leads to over-discharging, as it could harm the health of the BES. Thus, we modeled the entire microgrid and simulated the consequence of DoS under insufficient energy storage in the simulator PowerWorld. As shown in Fig. 18, the battery in the BES system is depleted in the absence of PV input for a while, and the frequency of the microgrid decreases rapidly, leading to a power outage (according to the IEEE Std 1547-2003 [11], in microgrids, the frequency deviation should not be greater than 5% of nominal). Note that as long as the PV output power is less than the load power, the BES system will continue to discharge, ultimately leading to a power outage of the microgrid.

C. Influence Quantification

Based on the principle of EMI, the EMI distance and power can influence the ReThink threat. In this subsection, we analyze the influence of EMI distance and power on ReThink under the threat model.

1) Influence of EMI Distance and Power on Inverter Sensors: Here, we evaluate the effects of ReThink on the deviation of the DC bus voltage ΔV_{dc} at $0 \sim 215$ cm, using 5 W, 10 W, 20 W and 50 W as the total power. The result is depicted in Fig. 19(a). We can see that higher power allows for a greater working distance. Taking the C2000 PV inverter as an instance, the self-protection mechanism will be triggered when the V_{dc} suddenly changes by 30 V. With a 20 W EMI device, the inverter can be affected at a distance of around 150 cm.

We placed the antenna at distances of 50 cm and 100 cm from the target PV inverter and tested the effects of power on the deviation of the DC bus voltage ΔV_{dc}. The result is shown in Fig. 19(b). For the adversary's target to generate a 30 V offset on ΔV_{dc}, when the distance is 50 cm, the adversary only needs an EMI power of 5 W.

2) Influence of EMI Distance and Power to DoS the Commercial Inverter: Since commercial inverters respond similarly to EMI, we chose a well-selling commercial inverter, Kstar BluE-G, and recorded the maximum distance to perform DoS at a specific power. As shown in Fig. 19(c), we can see that a 20 W EMI can achieve DoS at a distance of 160 cm, consistent with our threat model.

VI. Discussion

In this section, we analyze the limits, diversity, and countermeasures of ReThink, and design a portable and cost-effective EMI device to show its practicality.

A. Limits of ReThink

1) Subject to Power and Distance: The EMI power and distance are crucial impact factors of ReThink. Essentially,

TABLE II. RESULT OF ReThink ON PV INVERTERS.

Inverter	DoS						Damage			Damping			
	On DC side			On AC side			Pow. (W)	Freq. (MHz)	Result	Freq. (MHz)	Pow.(W) before Damping	Pow.(W) after Damping [2]	Pow. dev. rate
	Pow. (W)	Freq. (MHz)	Success rate[1]	Pow. (W)	Freq.(MHz) Pos./Neg.[4]	Success rate[1]							
Ti C2000	5	735	100%	5	1036/1490	100%	10	1000	100%	760	80	30	62.5%
Ginlong	10	916	100%	10	625/1210	80%	-[3]	-	-	1192	1980	1830	7.6%
Kstar	10	749	100%	10	990/810	90%	-	-	-	998	1995	1890	5.3%
Huawei[5]	10	1150	100%	10	980/1020	80%	-	-	-	1330	1960	1850	5.6%
GW(LCD,50kW)	20	920	100%	-	-	-	-	-	-	960	35.6k	2k	94.3%
GW(LED,60kW)[6]	20	945	100%	-	-	-	-	-	-	-	-	-	-

[1] For DoS on each inverter, we repeat the experiment 10 times from different angles and calculate the success rate.
[2] For Damping, we repeat the experiment 10 times and calculate the average deviation.
[3] "-" means there is no result (Considering safety or other factors).
[4] "Pos./Neg." means the positive and negative deviation; "Pow." means power; "Freq." means frequency.
[5] For Huawei SUN2000, all the experiments were done with the shell removed, we will give detailed reasons in Section VI.
[6] For Goodwe(LED,60kW) inverter, we don't perform Damping because there is no LCD screen to display the power.

our work represents one type of attacks exploiting analog signals. Such analog attacks have to follow the law of physics and a larger impact distance requires a more powerful transmitter. Notably, we find that DoS has great upward compatibility with power. For example, if a 10 W EMI signal at 50 cm can shut down the inverter, then EMI signals with 20 W, 30 W or even 50 W can achieve the same effect. The adversary shall choose the highest possible power for success. For exploitability, attackers can disguise themselves as a passerby or remotely control drones carrying our designed portable devices, as demonstrated in video [2].

2) Limited Impact Scale: Different from cyber-attacks that may cause large-scale outages, the impact of our attack is limited to PV inverters and potentially local PV microgrids. For a larger-scale grid, there may be greater resilience to compensate for the PV power. Thus, for attackers with different goals, EMI may not always be the best approach. Besides, attackers with physical access to the inverter may launch simpler attacks with more predictable consequences. Nonetheless, EMI attacks can be stealthier than cyberattacks in terms of digital traces, and they are also safer for attackers compared with direct physical attacks. We believe ReThink is applicable to local microgrid-scale attack scenarios where the attack needs to be stealthy and difficult to trace back.

B. Diversity of ReThink

1) Diversity of the Impact: We propose DoS, Damage, and Damping to illustrate the threat of ReThink. Since EMI can control multiple sensors simultaneously, adversaries can use it to explore more impacts, such as controlling the output frequency, the output power factor, and more. For example, EMI can also introduce harmonics (using the method in Fig. 11) into the AC output of the inverter and damage electrical appliances or devices.

2) Diversity of the Victim: This study highlights the vulnerability of op-amp-based voltage and current sensors in PV inverters to EMI. While PV inverter is a typical example of power electronic devices, the scope of potential victims can extend. Similar sensor technologies and energy conversion processes are prevalent in various applications, including power grids, electric vehicles, and industrial machinery. Additionally, the control algorithms employed in different inverters partly exhibit similar characteristics. For instance, the battery storage inverter may adopt the TSPC system [47], implying the presence of a DC bus capacitor in such inverters and the associated impact of Damage and DoS. Consequently, it is imperative that the security analysis by ReThink should also be performed in these diverse domains.

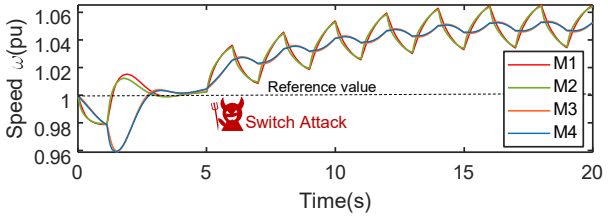


Fig. 20. The simulation result of Switching Attack with Damping.

C. Exploitability of ReThink

ReThink may cause consequences to the microgrid that go beyond those achieved in our evaluation, under specific conditions where there are both solar PV and synchronous generators in a grid. Particularly, for the Damping that can manipulate the output power of PV inverter by more than 90% (as tested in the real-world microgrid), it can launch in an on/off pattern and induce low-frequency oscillations of power supplies, which may cause physical damage of other synchronous generators and even result in a power outage, similar to how Switching Attacks [37] affect the grids [25]. This is because, the low-frequency oscillations can result in angular speed oscillations of generators, which can lead to damage or disconnecting of the generators. It has been demonstrated that manipulating a mere 1.23% of the total system power is enough to achieve the Switching Attack [28]. To further verify, we simulate the use of Damping to oscillate the angular velocity of generators in the grid (the modified Kundur benchmark system with four synchronous generators and two PV farms [50]) via Simulink, and our simulation result shows that Damping could cause this cascading failure effectively, as shown in Fig. 20.

D. Countermeasures

1) Vulnerability of Filtering Leakage and Corresponding Countermeasures: ① **Filtering of Ultra-high Frequency (UHF) Noise.** Low-pass filtering is often employed for the suppression of high-frequency interference. However, the low-pass filter in practice shows leakage at UHF noise, as

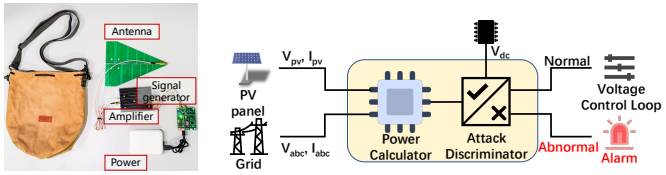
shown in Fig. 31. For low-pass filters composed of inductors and capacitors, leakage occurs when the input signal frequency is much higher than the filter cut-off frequency [46].

A potential countermeasure is to design filters for different frequency bands of interference. The three-stage low-pass filter structure has better performance in dealing with high disturbance of UHF noise, with a low-frequency bandwidth of $10\,\mathrm{kHz} \sim 1\,\mathrm{MHz}$, medium frequency bandwidth of $1\,\mathrm{MHz} \sim 100\,\mathrm{MHz}$, and high-frequency bandwidth of $100\,\mathrm{MHz} \sim 1\,\mathrm{GHz}$ (Fig. 32 in Appendix C).

② **Shielding Against Ultra-high Frequency Noise.** The filtering effect of low-pass filter circuits on Ultra-high noise is limited by its physical characteristics. According to Table II, we have evaluated 5 off-the-shelf PV inverters, all of which have EMC-proof metal-case shielding. However, SUN2000 is the only inverter whose shielding is "effective" in resisting `ReThink` within the threat model. To explore, we sawed and deconstructed 3 commercial PV inverters to compare their cases (Fig. 33 in Appendix C) and found different thicknesses of metal cases ($4\,\mathrm{mm}$ on SUN2000 and $2\,\mathrm{mm}$ on others). All of them meet the IP65 standard requirement according to the International Organization for Standardization ISO 20653:2023 [23] and International Electrotechnical Commission IEC 60529 [10]: with a thickness of 2 mm and waterproof silicone gasketsand. To further investigate how to strengthen the enclosures, we simulated the shielding effectiveness of 4 kinds of common shielding metals in COMSOL. According to our simulation in Fig. 34 and Fig. 35 of Appendix E, all enclosures above $2\,\mathrm{mm}$ thickness can meet the requirements of aerospace and military, but thicker enclosures can achieve better effects, such as resisting intentional EMI attacks. Additionally, we find that the LCD screens and cable interfaces may serve as entry points for external EMI. In our evaluation, only Huawei inverter [31] adopts an LED display and can resist EMI. Previous work [5] suggests that the number of holes should be increased and the size of each hole should be reduced. For the PV inverters, we recommend using LED displays instead of LCDs and designing the cable interface with a metal connector to better block EMI.

2) Consistency Checking for Anomaly Detection: Since the PV inverter is a relatively "stable" system, there is often a relation between the sensors inside the PV inverter, due to the properties of power electronics. It is difficult for an adversary to fully follow the hidden "rules" when tampering with multiple sensors. Therefore, manufacturers can design a consistency checking algorithm.

The threat of `ReThink` also exploits the vulnerability in the control algorithm, which can be avoided in the controller design. For instance, the strategy to ensure the same input and output power of the entire inverter is to keep the DC bus voltage unchanged. The current control algorithm has no power information input from the PV panel to the inverter, and hence the adversary can manipulate the voltage by spoofing the DC bus voltage sensor. Fig. 21(b) presents a solution. This method inputs the voltage/current of the DC side and the AC side into the voltage control loop to calculate the input and output power on the capacitor C_{dc} and compares it with the capacitor voltage V_{dc} received by the voltage sensor. If the changes are consistent, it indicates that the DC bus voltage sensor is not under threat; otherwise, the inverter should issue an alarm.



(a) Portable device. (b) Vulnerability repair of voltage control.

Fig. 21. Portable devices and control vulnerability repair.

E. Portable and Cost-effective EMI Devices

We design a portable EMI device in Fig. 21(a). We select a mobile power with a maximum output of $5\ V$ and $3\ A$ and a cost of \$8. We select LTDZ MAX2870 [22] based on STM32 as the signal source that can generate signals in $23.5 \sim 6000\,\mathrm{MHz}$, with a cost of \$45. Based on the result in Fig. 19(c), we choose a portable amplifier [71] with $10\,\mathrm{W}$ power, costing \$95. We then use an LS200-150 log-periodic antenna with a cost of \$9 to emit EMI signals. The entire device costs \$157 in total and can be hidden in a shoulder bag. Finally, we successfully use the portable device to implement `DoS` impact on commercial inverter [42]; see demo video [2].

VII. Related Works

EMI attacks against sensors, actuators and communications have been studied extensively [43], [35], [94], [12], [73], [68], [49], [86], [69], [39], [34]; the detailed comparison can be seen in Table III of Appendix D. These best practices inspire us in the EMI attack design, such as determining the carrier frequency via frequency-sweep tests and modulating attack signals using amplitude modulation. In comparison, ① to the best of our knowledge, we are the first to investigate the principle of achieving fine-grained incremental and decremental output control on differential op-amp-based sensors with EMI. We find and verify that the asymmetric layout of the differential input lines weakens the common-mode rejection function, and the amplified survival error can cause both incremental and decremental changes to the sensor output; ② we show the feasibility of manipulating complicated and robust control algorithms with EMI attacks. For instance, we propose new techniques for bypassing the Clarke/Park transformation and spoofing the MPPT algorithms. However, techniques commonly used in prior work such as injecting a constant deviation or random disruption to the sensor readings may fail to achieve `DoS` or `Damping`, as shown in Fig. 24 of Appendix A and Fig. 27 of Appendix B; ③ we verify that the current inverters' enclosures need to be improved to cope with the intentional EMI concerns.

Current research on defense against EMI includes passive defense based on shielding [24], [41], [79], [88] and filtering [96], [89], [48], and active defense based on detection. Active defense includes ① adding extra detection circuits to detect EMI [1], [2], [13], [84], [97], ② encoding critical signals secretly to detect EMI [39], [64], [74], and ③ designing algorithm based on sensor characteristics to detect EMI [21], [35], [36], [56], [87]. The detailed comparison of these works is shown in Table IV of Appendix D. In conclusion, the passive defense methods can thoroughly eliminate the EMI threats with additional hardware costs; the active defense methods can typically detect `ReThink` with lower costs, although there is

a lack of effective ways to actively eliminate the impact of EMI after they are detected, which we believe is a direction of future work.

VIII. Conclusion

In this paper, we systematically analyze the security of PV inverters and reveal the threat of EMI on both voltage and current sensors of PV inverters. We analyze the threat `ReThink` and identify three destructive impacts, `DoS`, `Damage`, and `Damping`, which can cause the victim PV inverter to shut down, physically burn out, and reduce output power, respectively. The evaluations are successfully conducted on an inverter development kit, 5 off-the-shelf PV inverters and a real-world microgrid. Finally, we discuss the limits, diversity, exploitability and countermeasures of the threat. We hope our work can raise awareness of the security of power electronic devices in the grids with increasing RES. The observations could also facilitate the security analysis of other types of power electronic devices.

Acknowledgment

We thank the anonymous reviewers for their valuable comments. This work is supported by the National Natural Science Foundation of China under Grant 62201501, 52161135201, 62201503, 61925109, 62222114, and 62071428.

References

[1] C. Adami, C. Braun, P. Clemens, M. Jöster, S. Ruge, M. Suhrke, H. U. Schmidt, and H.-J. Taenzer, "Hpm detector system with frequency identification," in 2014 International Symposium on Electromagnetic Compatibility. IEEE, 2014, pp. 140–145.

[2] C. Adami, C. Braun, P. Clemens, M. Suhrke, H. Schmidt, and A. Taenzer, "Hpm detection system for mobile and stationary use," in 10th International Symposium on Electromagnetic Compatibility. IEEE, 2011, pp. 1–6.

[3] C. S. Analysis. (2022) Emi types and coupling methods. [Online]. Available: https://resources.system-analysis.cadence.com/blog/msa2022-emi-types-and-coupling-methods

[4] Baekhyn0506, "Characteristics and diagramming of operational amplifier circuits," [EB/OL], 2022, https://www.elecfans.com/analog/202208161878428.html.

[5] Z. Y. Bai Wanning, L. Y. Liu QiangQiang, and Q. We, "Research on electromagnetic shielding characteristics of switching power supply enclosure based on hole slot design," Journal of Nanjing Normal University (Engineering and Technology Edition), 2019.

[6] A. Barua and M. A. Al Faruque, "Hall spoofing: A non-invasive dos attack on grid-tied solar inverter," in 29th USENIX Security Symposium (USENIX Security 20), 2020, pp. 1273–1290.

[7] H. Benkraouda, M. A. Chakkantakath, A. Keliris, and M. Maniatakos, "Snifu: Secure network interception for firmware updates in legacy plcs," in 2020 IEEE 38th VLSI Test Symposium (VTS). IEEE, 2020, pp. 1–6.

[8] M. Biglarbegian, S. J. Nibir, H. Jafarian, and B. Parkhideh, "Development of current measurement techniques for high frequency power converters," in 2016 IEEE International Telecommunications Energy Conference (INTELEC), 2016, pp. 1–7.

[9] Z. Chen, M. Ding, and J. Su, "Modeling and control for large capacity battery energy storage system," in 2011 4th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT). IEEE, 2011, pp. 1429–1436.

[10] I. E. Commission. (2013) Degrees of protection provided by enclosures (ip code). [Online]. Available: https://webstore.iec.ch/publication/2452

[11] I. S. C. Committee et al., "1547.4-2011-ieee guide for design, operation, and integration of distributed resource island systems with electric power systems," 2011.

[12] D. Dai, Z. An, and L. Yang, "Inducing wireless chargers to voice out for inaudible command attacks," in 2023 IEEE symposium on security and privacy (SP). IEEE, 2023, pp. 1789–1806.

[13] J. Dawson, I. Flintoft, P. Kortoci, L. Dawson, A. Marvin, M. Robinson, M. Stojilovic, M. Rubinstein, B. Menssen, H. Garbe et al., "A cost-efficient system for detecting an intentional electromagnetic interference (iemi) attack," in 2014 International Symposium on Electromagnetic Compatibility. IEEE, 2014, pp. 1252–1256.

[14] G. Y. Dayanıklı, S. Sinha, D. Muniraj, R. M. Gerdes, M. Farhood, and M. Mina, "Physical-Layer attacks against pulse width Modulation-Controlled actuators," in 31st USENIX Security Symposium (USENIX Security 22). Boston, MA: USENIX Association, Aug. 2022, pp. 953–970. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/dayanikli

[15] A. Devices. (2009) Rfi rectification concepts. [Online]. Available: https://www.analog.com/media/en/training-seminars/tutorials/MT-096.pdf

[16] R. Dogga and M. Pathak, "Recent trends in solar pv inverter topologies," Solar Energy, vol. 183, pp. 57–73, 2019.

[17] S. Dong, E. Kremers, M. Brucoli, S. Brown, and R. Rothman, "Residential pv-bes systems: Economic and grid impact analysis," Energy procedia, vol. 151, pp. 199–208, 2018.

[18] F. R. O. Eero Vartiainen. Lcoe and competitiveness - etip pv. [Online]. Available: https://etip-pv.eu/about/working-groups/lcoe-competiveness/

[19] N. S. Electric. (2023) Inverter basics and selecting the right mode. [Online]. Available: https://www.solar-electric.com/learning-center/inverter-basics-selection.html/

[20] L. Fan, A. Knott, and I. H. H. Jørgensen, "Layout capacitive coupling and structure impacts on integrated high voltage power mosfets," in 2016 12th Conference on Ph.D. Research in Microelectronics and Electronics (PRIME), 2016, pp. 1–4.

[21] K. Fang, T. Wang, X. Yuan, C. Miao, Y. Pan, and J. Li, "Detection of weak electromagnetic interference attacks based on fingerprint in iiot systems," Future Generation Computer Systems, vol. 126, pp. 295–304, 2022.

[22] S. B. S. S. E. Firm. Ltdx max2870. [Online]. Available: https://www.alibaba.com/product-detail/MAX2870-23-5-6000MHz-0-96_1600594901578.html?spm=a2700.galleryofferlist.normal_offer.d_image.27c6a4f3SyzgVR

[23] I. O. for Standardization. (2023) Degrees of protection (ip code) protection of electrical equipment against foreign objects, water and access. [Online]. Available: https://www.iso.org/standard/76116.html

[24] S. Geetha, K. Satheesh Kumar, C. R. Rao, M. Vijayan, and D. Trivedi, "Emi shielding: Methods and materials—a review," Journal of applied polymer science, vol. 112, no. 4, pp. 2073–2086, 2009.

[25] M. Ghafouri, E. Kabir, B. Moussa, and C. Assi, "Coordinated charging and discharging of electric vehicles: A new class of switching attacks," ACM Transactions on Cyber-Physical Systems (TCPS), vol. 6, no. 3, pp. 1–26, 2022.

[26] L. Ginlong Technologies Co. (2022, Nov.) Solis s6 single phase inverter. [Online]. Available: https://www.ginlong.com/uploads/file/Solis_Manual_S6-GR1P(2,5-6)K_FN_EUR_V1,2(20221116).pdf

[27] L. GoodWe Technologies Co. (2023, Dec.) Goodwe gw50k-mt. [Online]. Available: https://en.goodwe.com/Ftp/EN/Downloads/User%20Manual/GW_MT_User%20Manual-EN.pdf

[28] E. Hammad, A. M. Khalil, A. Farraj, D. Kundur, and R. Iravani, "A class of switching exploits based on inter-area oscillations," IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4659–4668, 2017.

[29] ——, "A class of switching exploits based on inter-area oscillations," IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4659–4668, 2018.

[30] A. Harrag and S. Messalti, "Variable step size modified p&o mppt algorithm using ga-based hybrid offline/online pid controller," Renewable and Sustainable Energy Reviews, vol. 49, pp. 1247–1260, 2015.

[31] L. Huawei Technologies Co. (2024) Fusionsolar. [Online]. Available: https://solar.huawei.com/eu/Products/FusionSolar

[32] ——. (2024, Jan.) Huawei sun2000-2/3/3.68/4/4.6/5/6ktl-l1. [Online]. Available: https://solar.huawei.com/hu-HU/download?p=%2F-%2Fmedia%2FSolar%2Fattachment%2Fpdf%2Feu%2Fdatasheet%2FSUN2000-2-6KTL-L1.pdf

[33] M. Islam, S. Mekhilef, and M. Hasan, "Single phase transformerless inverter topologies for grid-tied photovoltaic system: A review," Renewable and sustainable energy reviews, vol. 45, pp. 69–86, 2015.

[34] Q. Jiang, X. Ji, C. Yan, Z. Xie, H. Lou, and W. Xu, "{GlitchHiker}: Uncovering vulnerabilities of image signal transmission with {IEMI}," in 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 7249–7266.

[35] C. Kasmi and J. L. Esteves, "Iemi threats for information security: Remote command injection on modern smartphones," IEEE Transactions on Electromagnetic Compatibility, vol. 57, no. 6, pp. 1752–1755, 2015.

[36] C. Kasmi and J. Lopes-Esteves, "Automated analysis of the effects induced by radio-frequency pulses on embedded systems for emc functional safety," in 2015 1st URSI Atlantic Radio Science Conference (URSI AT-RASC). IEEE, 2015, pp. 1–1.

[37] B. J. Kirby, J. Dyer, C. Martinez, R. A. Shoureshi, R. Guttromson, J. Dagle et al., Frequency control concerns in the North American electric power system. United States. Department of Energy, 2003.

[38] B. F. Kjærsgaard, G. Liu, M. R. Nielsen, R. Wang, D. N. Dalal, T. S. Aunsborg, J. K. Jørgensen, Z. Yan, J. Jacobsen, R. Wu, M. M. Bech, B. Rannestad, S. Munk-Nielsen, and H. Zhao, "Parasitic capacitive couplings in medium voltage power electronic systems: An overview," IEEE Transactions on Power Electronics, vol. 38, no. 8, pp. 9793–9817, 2023.

[39] S. Köhler, R. Baker, and I. Martinovic, "Signal injection attacks against ccd image sensors," in Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, 2022, pp. 294–308.

[40] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic, "Brokenwire: Wireless disruption of ccs electric vehicle charging," arXiv preprint arXiv:2202.02104, 2022.

[41] S. B. Kondawar and P. R. Modak, "Theory of emi shielding," in Materials for potential emi shielding applications. Elsevier, 2020, pp. 9–25.

[42] L. Kstar Technologies Co. (2021, Mar.) String grid-tied pv inverterbiueg 3000d/4000d/5000d/5000d-au/6000d. [Online]. Available: https://www.kstar.com/cn/upload/cms/www/20210324170423587.PDF

[43] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in 2013 IEEE Symposium on Security and Privacy, 2013, pp. 145–159.

[44] R. H. Lasseter and P. Paigi, "Microgrid: A conceptual solution," in 2004 IEEE 35th annual power electronics specialists conference (IEEE Cat. No. 04CH37551), vol. 6. IEEE, 2004, pp. 4285–4290.

[45] Y. Li, S. Wang, H. Sheng, and S. Lakshmikanthan, "Reduction and cancellation techniques for the near field capacitive coupling and parasitic capacitance of inductors," in 2018 IEEE Symposium on Electromagnetic Compatibility, Signal Integrity and Power Integrity, 2018, pp. 432–437.

[46] H. X. Li Guishan, Yang Jianping, "The study of emi/rfi and its rejection," Proceedings of the EPSA, vol. 14, no. 4, pp. 36–44, 2002.

[47] M. Liu, X. Cao, C. Cao, P. Wang, C. Wang, J. Pei, H. Lei, X. Jiang, R. Li, and J. Li, "A review of power conversion systems and design schemes of high-capacity battery energy storage systems," IEEE Access, vol. 10, pp. 52 030–52 042, 2022.

[48] F. Luo, D. Boroyevich, and P. Mattavelli, "Improving emi filter design with in circuit impedance mismatching," in 2012 Twenty-Seventh Annual IEEE Applied Power Electronics Conference and Exposition (APEC). IEEE, 2012, pp. 1652–1658.

[49] S. Maruyama, S. Wakabayashi, and T. Mori, "Tap'n ghost: A compilation of novel attack techniques against smartphone touchscreens," in 2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019, pp. 620–637.

[50] MathWork. (2024) Performance of three pss for interarea oscillations. [Online]. Available: https://ww2.mathworks.cn/help/sps/ug/performance-of-three-pss-for-interarea-oscillations.html?searchHighlight=Kundur&s_tid=srchtitle_support_results_2_Kundur

[51] L. Mini-Circuits Technologies Co. High power amplifier hpa-50w-63+. [Online]. Available: https://www.minicircuits.com/pdfs/HPA-50W-63+.pdf

[52] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in 2009 47th annual Allerton conference on communication, control, and computing (Allerton). IEEE, 2009, pp. 911–918.

[53] A. Z. Mohammed, A. Singh, G. Y. Dayanıklı, R. Gerdes, M. Mina, and M. Li, "Towards wireless spiking of smart locks," in 2022 IEEE Security and Privacy Workshops (SPW). IEEE, 2022, pp. 251–257.

[54] S. Moosavian, N. Rahim, J. Selvaraj, and K. Solangi, "Energy policy to promote photovoltaic generation," Renewable and Sustainable Energy Reviews, vol. 25, pp. 44–58, 2013.

[55] S. Motahhir, A. El Hammoumi, and A. El Ghzizal, "The most used mppt algorithms: Review and the suitable low-cost embedded board for each algorithm," Journal of cleaner production, vol. 246, p. 118983, 2020.

[56] D. Muniraj and M. Farhood, "Detection and mitigation of actuator attacks on small unmanned aircraft systems," Control Engineering Practice, vol. 83, pp. 188–202, 2019.

[57] Y. Murata, K. Takahashi, T. Kanamoto, and M. Kubota, "Analysis of parasitic couplings in emi filters and coupling reduction methods," IEEE Transactions on Electromagnetic Compatibility, vol. 59, no. 6, pp. 1880–1886, 2017.

[58] U. D. of Energy. (2020) Heart turns brain. [Online]. Available: https://www.energy.gov/oe/grid-systems

[59] N. Panwar, S. Kaushik, and S. Kothari, "Role of renewable energy sources in environmental protection: A review," Renewable and sustainable energy reviews, vol. 15, no. 3, pp. 1513–1524, 2011.

[60] B. Parida, S. Iniyan, and R. Goic, "A review of solar photovoltaic technologies," Renewable and sustainable energy reviews, vol. 15, no. 3, pp. 1625–1636, 2011.

[61] Z. Qu, Z. Zhu, Y. Liu, M. Yu, and T. T. Ye, "Parasitic capacitance modeling and measurements of conductive yarns for e-textile devices," Nature Communications, vol. 14, no. 1, p. 2785, 2023.

[62] L. RIGOL Technologies Co. (2016, Apr.) Dp711 programmable liner dc power supply. [Online]. Available: https://beyondmeasure.rigoltech.com/acton/attachment/1579/f-06b5/1/-/-/-/-/DP700%20Data%20Sheet.pdf

[63] ——. (2021, Apr.) Rp1000d series high voltage differential probe. [Online]. Available: https://beyondmeasure.rigoltech.com/acton/attachment/1579/f-01c6/1/-/-/-/-/file.pdf

[64] H. Ruotsalainen, A. Treytl, and T. Sauter, "Watermarking based sensor attack detection in home automation systems," in 2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). IEEE, 2021, pp. 1–8.

[65] S. Sahoo, J. C.-H. Peng, A. Devakumar, S. Mishra, and T. Dragičević, "On detection of false data in cooperative dc microgrids—a discordant element approach," IEEE Transactions on Industrial Electronics, vol. 67, no. 8, pp. 6562–6571, 2019.

[66] M. Sarvi and A. Azadian, "A comprehensive review and classified comparison of mppt algorithms in pv systems," Energy Systems, vol. 13, no. 2, pp. 281–320, 2022.

[67] J. Selvaraj, G. Y. Dayanıklı, N. P. Gaunkar, D. Ware, R. M. Gerdes, and M. Mina, "Electromagnetic induction attacks against embedded systems," in Proceedings of the 2018 on Asia Conference on Computer and Communications Security, 2018, pp. 499–510.

[68] ——, "Electromagnetic induction attacks against embedded systems," in Proceedings of the 2018 on Asia Conference on Computer and Communications Security, 2018, pp. 499–510.

[69] H. Shan, B. Zhang, Z. Zhan, D. Sullivan, S. Wang, and Y. Jin, "Invisible finger: Practical electromagnetic interference attack on touchscreen-based electronic devices," in 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022, pp. 1246–1262.

[70] V. K. Sharma, R. Singh, A. Gehlot, D. Buddhi, S. Braccio, N. Priyadarshi, B. Khan et al., "Imperative role of photovoltaic and concentrating solar power technologies towards renewable energy generation," International Journal of Photoenergy, vol. 2022, 2022.

[71] L. Shenzhen Bochuang Spacetime Communication Technology Co. (2024, Jan.) Portable amplifier. [Online]. Available: https://www.alibaba.com/product-detail/10-watt-2-4G-frequency-band_1600916555222.html?spm=a2700.galleryofferlist.normal_offer.d_title.47c270e3SCJ428

[72] L. Shenzhen Shengda Communication Equipment Co. The 5g directional antenna. [Online]. Available: https://www.alibaba.com/product-detail/High-Gain-Waterproof-Outdoor-800-2500MHZ_62344368753.html?spm=a2700.galleryofferlist.normal_offer.d_title.3a957fb11mPRbq

[73] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in Cryptographic Hardware and Embedded Systems-CHES 2013: 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings 15. Springer, 2013, pp. 55–72.

[74] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "Pycra: Physical challenge-response authentication for active sensors under spoofing attacks," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015, pp. 1004–1015.

[75] A. Soni. (2023) What is electromagnetic coupling? [Online]. Available: https://www.ansys.com/blog/saving-chips-from-electromagnetic-coupling#:~:text=The%20electric%20field%20component%20is,charge%20to%20the%20victim%20conductor.

[76] L. SUNGROW Technologies Co. (2023) String inverter of sungrow. [Online]. Available: https://en.sungrowpower.com/ProductsHome/14/16/string-inverter

[77] K. Technologies. (2023, Feb.) Exg x-series signal generators n5171b analog & n5172b vector. [Online]. Available: https://www.keysight.com/us/en/assets/7018-03381/data-sheets/5991-0039.pdf

[78] L. TEWERD Technologies Co. Tewerd tpv1000. [Online]. Available: https://www.tewerd.com/PVsimulator.html

[79] J.-M. Thomassin, C. Jérôme, T. Pardoen, C. Bailly, I. Huynen, and C. Detrembleur, "Polymer/carbon based composites as electromagnetic interference (emi) shielding materials," Materials Science and Engineering: R: Reports, vol. 74, no. 7, pp. 211–232, 2013.

[80] L. Ti Technologies Co. (2014, Sep.) C2000 solar micro inverter quick start guide. [Online]. Available: https://www.ti.com/lit/pdf/tidu406

[81] ——. (2014, Sep.) Grid-tied solar micro inverter with mppt schematic (rev. a). [Online]. Available: https://www.ti.com/lit/pdf/tidr767

[82] L. TMEIC Technologies Co. (2023) Pv inverters. [Online]. Available: https://www.tmeic.com/products/pv-inverters

[83] Y. Tu, S. Rampazzi, B. Hao, A. Rodriguez, K. Fu, and X. Hei, "Trick or heat? attack on amplification circuits to abuse critical temperature control systems," arXiv preprint arXiv:1904.07110, 2019.

[84] Y. Tu, V. S. Tida, Z. Pan, and X. Hei, "Transduction shield: A low-complexity method to detect and correct the effects of emi injection attacks on sensors," in Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, 2021, pp. 901–915.

[85] H. Wang, J. Ruan, Z. Ma, B. Zhou, X. Fu, and G. Cao, "Deep learning aided interval state prediction for improving cyber security in energy internet," Energy, vol. 174, pp. 1292–1304, 2019.

[86] K. Wang, R. Mitev, C. Yan, X. Ji, A.-R. Sadeghi, and W. Xu, "{GhostTouch}: Targeted attacks on touchscreens without physical touch," in 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 1543–1559.

[87] ——, "Ghosttouch: Targeted attacks on touchscreens without physical touch," in 31st USENIX Security Symposium (USENIX Security 22). USENIX Association, Boston, MA. https://www.usenix.org/conference/usenixsecurity22/presentation/wang-kai, 2022.

[88] L. Wang, Z. Ma, Y. Zhang, L. Chen, D. Cao, and J. Gu, "Polymer-based emi shielding composites with 3d conductive networks: a mini-review," SusMat, vol. 1, no. 3, pp. 413–431, 2021.

[89] S. Wang, F. C. Lee, D. Y. Chen, and W. G. Odendaal, "Effects of parasitic parameters on emi filter performance," IEEE transactions on power electronics, vol. 19, no. 3, pp. 869–877, 2004.

[90] W. Westerhof. (2017) Horus scenario. [Online]. Available: https://horusscenario.com/

[91] Wikimedia. (2024, Jan.) Power inverter. [Online]. Available: https://en.wikipedia.org/wiki/Power_inverter

[92] H. Wu, J. Fang, and H. Tang, "Study on emc of high power photovoltaic grid-connected inverter," in High Power Converter Technology, 2014, pp. 60–79.

[93] Z. Xie, C. Yan, X. Ji, and W. Xu, "Bitdance: Manipulating uart serial communication with iemi," in Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses, 2023, pp. 63–76.

[94] Z. Xu, R. Hua, J. Juang, S. Xia, J. Fan, and C. Hwang, "Inaudible attack on smart speakers with intentional electromagnetic interference," IEEE Transactions on Microwave Theory and Techniques, vol. 69, no. 5, pp. 2642–2650, 2021.

[95] Y. Yang, Y. Ruan, H.-q. Shen, Y.-y. Tang, and Y. Yang, "Grid-connected inverter for wind power generation system," Journal of Shanghai University (English Edition), vol. 13, no. 1, pp. 51–56, 2009.

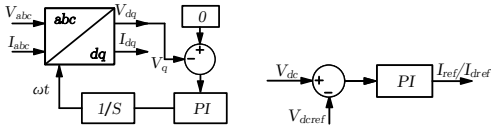
[96] S. Ye, W. Eberle, and Y.-F. Liu, "A novel emi filter design method for switching power supplies," IEEE Transactions on Power Electronics, vol. 19, no. 6, pp. 1668–1678, 2004.

[97] Y. Zhang and K. Rasmussen, "Detection of electromagnetic signal injection attacks on actuator systems," in Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses, 2022, pp. 171–184.

APPENDIX

A. Control Algorithms in Simulations

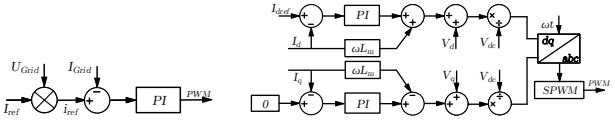
This section gives the control algorithm in simulations, where Fig. 22(a) shows the control algorithm for PLL, Fig. 22(b) shows the voltage control loop, Fig. 23(a) shows the current control loop for single-phase PV inverters, Fig. 23(b) shows the current control loop for three-phase PV inverters.



(a) Control algorithm of PLL.

(b) Control algorithm of voltage control loop.

Fig. 22. Control algorithms of PLL and voltage control.



(a) Control algorithm of single-phase current control loop.

(b) Control algorithm of three-phase current control loop.

Fig. 23. Control algorithms of the single-phase and three-phase current control loop.

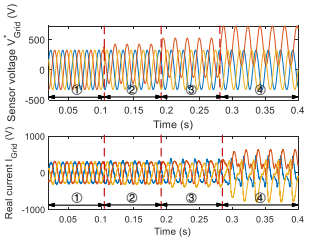


Fig. 24. Inject the signal into one phase of the voltage sensor. ①:$V_a = 0V$, ②:$V_a = 50V$, ③:$V_a = 100V$, ④:$V_a = 200V$.

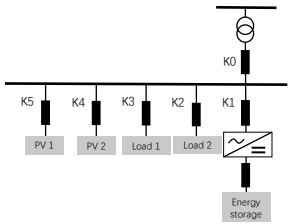
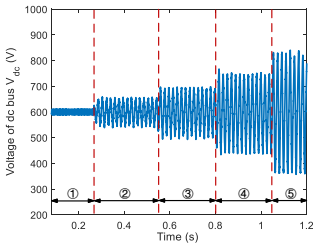
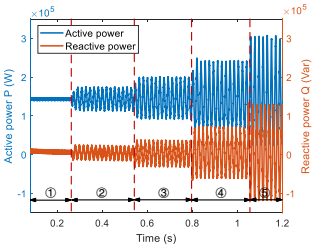


Fig. 25. The structure of the micro-grid we evaluated.

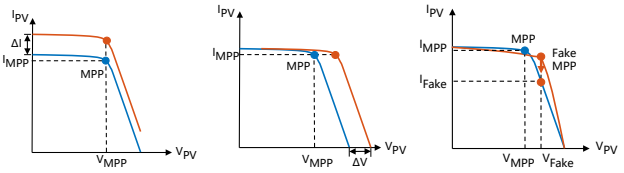


(a) DC bus voltage. ①:$I_a = 0A$, ②:$I_a = 50A$, ③:$I_a = 100A$, ④:$I_a = 200A$, ⑤:$I_a = 400A$.



(b) Active/reactive power output. ①:$I_a = 0A$, ②:$I_a = 50A$, ③:$I_a = 100A$, ④:$I_a = 200A$, ⑤:$I_a = 400A$.

Fig. 26. The effect of system oscillations. Effect of system oscillations on DC bus voltage and output active/reactive power when the inverter protection is not set or is not triggered.



(a) Constant ΔI injection. (b) Constant ΔV injection. (c) Fake V-I curve injection.

Fig. 27. Different measurement manipulations on the V-I curve: (a) Inject a constant ΔI on the current measurement (b) Inject a constant ΔV on the voltage measurement;(c) Inject ΔI and ΔV by a specially designed V-I curve.

B. Simulation of Grid Sensor Tampering

1) Grid Voltage Sensor Tampering: We have given the simulation result of manipulating the current sensor in Fig. IV-C. Here we introduce the simulation result of manipulating the grid voltage sensor in this section. Figure 24 gives the impact by injecting a constant signal into one phase of the voltage sensor, the effect is similar to that when manipulating the current sensor. Note that the effect is still reflected in the grid current since the grid voltage is unaffected by controls (grid voltage is generally stable and not controlled by individual inverters).

2) Effect of Not Triggering Inverter Protection: The impact of system oscillations on the inverter and the grid under EMI on the grid voltage/current sensor is given in this section, considering that some inverters do not have adequate protection mechanisms in place or that the protection is not triggered under EMI. The specific manifestations of system oscillations under EMI on the inverter are two main aspects:

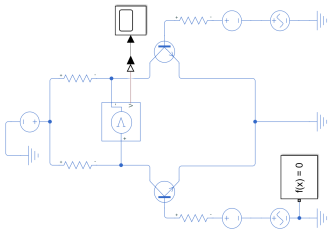


Fig. 28. The simulation model of the differential amplification input stage of op-amp chip in Simulink.

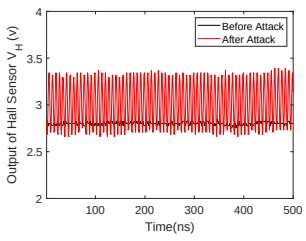


Fig. 29. The output of Hall current chip under EMI.

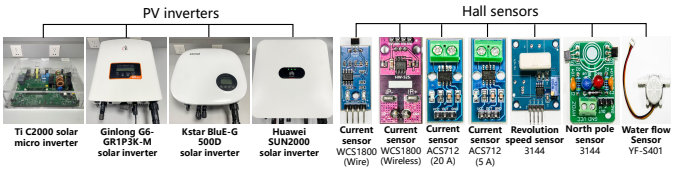


Fig. 30. The victim inverters and sensors we evaluated.

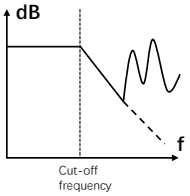


Fig. 31. Leakage of the single-stage low-pass filter.

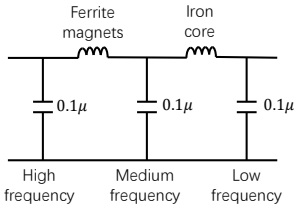


Fig. 32. Multi-stage filter.

DC bus voltage. The DC bus voltage V_{Bus} oscillates violently, as shown in Fig. 26(a). Due to the system oscillation, the inverter output power is unstable, resulting in the DC bus capacitor C_{Bus} constantly charging and discharging, which cannot be stabilized at the reference voltage.

Output power. The output active power oscillates and reactive power is injected into the grid, as shown in Fig. 26(b). The quality of grid-connected power drops significantly.

C. Supplementary Experimental Results

Simulation and experiment of EMI on voltage and current sensors. The simulation model of the differential amplification input stage of the op-amp chip is shown in Fig. 28. The result of the EMI on Hall chip is shown in Fig. 29.

The victim inverter, sensors and microgrid. The tested off-the-shelf PV inverters and Hall sensors are shown in Fig. 30. The structure of the tested micro-grid is shown in Fig. 25.

The filter leakage and corresponding countermeasures. We show the filter leakage of a low-pass filter in Fig.31 and a potential countermeasure using a multi-order filter in Fig.32.

The comparison of cases of 3 commercial PV inverters. We display the result of the disassembly and comparison of the cases of 3 commercial PV inverters in Fig. 33.

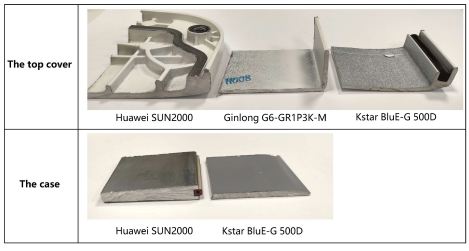


Fig. 33. The thickness of 3 commercial inverters' cases.

D. The Comparision with Previous EMI Works

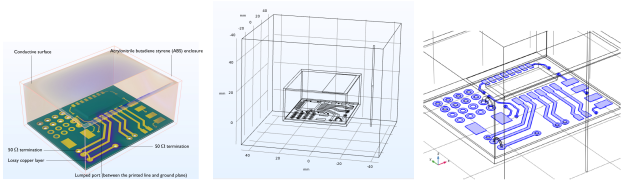
1) Comparision with previous EMI works: The detailed comparison of EMI attack works is shown in Table III, and

TABLE III. COMPARISON WITH PREVIOUS EMI WORKS

Work	Attack Target		Attack Method			Attack Capability		
	Victim	Signal Type	Attack Frequency	Utilize Victim's Amplifier	Analyse Control Algorithms	Attack Power (W)	Attack Distance (m)	Attack Effect
[43]	Microphone	Analog	826 MHz	✓	✗	10	$1 \sim 2$	Voice Command Injection
[94]	Microphone	Analog	$8 \sim 16$ GHz	✓	✗	2.5	2.5	Voice Command Injection
[73]	Magnetic sensor	Digital	500 Hz	✗	✗	/	/	Spoof wheel speed sensor
[68]	Embedded system	Digital	$170 \sim 320$ MHz	✗	✗	1.8	10	Manipulated analog and digital signals
[83]	Temperature sensor	Analog	$810 \sim 950$ MHz	✓	✗	3	3	Manipulate temperature sensors
[49]	Touchscreen	Digital	$60 \sim 90$ kHz	✗	✗	6	0.02	Manipulate touchscreen
[87]	Touchscreen	Digital	$46 \sim 86$ MHz	✗	✗	/	0.04	Manipulate touchscreen
[69]	Touchscreen	Digital	140 kHz	✗	✗	/	$0.7 \sim 2$	Manipulate touchscreen
[39]	CCD image sensor	Digital	190 MHz	✗	✗	0.1	0.3	Manipulate CCD image sensor
[34]	Camera signal line	Digital	1 GHz	✗	✗	/	0.3	Manipulate camera signal transmission
[53]	Smart lock	Digital	500 kHz	✗	✗	/	0.05	Unlock the smart lock
[40]	Charging system	Digital	/	✗	✗	1	47	DoS communication between charger and vehicle
[93]	UART serial	Digital	15.36 MHz	✗	✗	/	0.05	UART signal bit flip
[14]	Servo	Digital	$8 \sim 140$ MHz	✗	✗	20	0.5	DoS & Control servo
Our work	PV inverter	Analog	$735 \sim 1150$ MHz	✓	✓	20	1.5	DoS & Damage & Damp

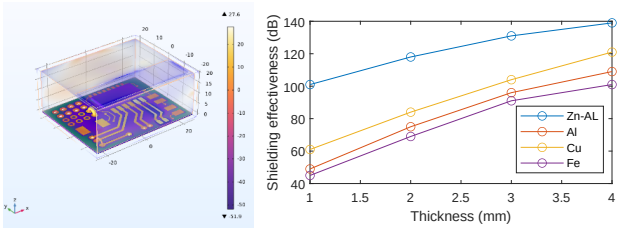
TABLE IV. COMPARISON OF DIFFERENT DEFENSE METHODS AGAINST EMI ATTACKS.

Type		**Work(s)**	**Detect EMI**	**Resist EMI**	**No Additional Circuit**	**No Additional Computation**	**No Additional Cost**
Active Defense (Detect EMI)	Add extra detection circuit	[1], [2], [13], [84], [97]	✓	✗	✗	✓	✗
	Encode critical signals secretly	[39], [64], [74]	✓	✗	✓	✗	✓
	Design algorithm based on sensor characteristics	[21], [35], [36], [56], [87]	✓	✗	✓	✗	✓
Passive Defense (Shielding and Filtering EMI)	Shielding EMI	[24], [41], [79], [88]	✗	✓	✓	✓	✗
	Filtering EMI	[96], [89], [48]	✗	✓	✗	✓	✗



(a) The enclosure. (b) The placement. (c) The EMI noise test points on PCB.

Fig. 34. The simulation model in COMSOL.



(a) Electromagnetic field distribution. (b) Shielding effectiveness.

Fig. 35. Simulation result of the shielding effectiveness under different thicknesses.

the comparison of EMI defense works is shown in Table IV.

2) Comparision with HallSpoofing: HallSpoofing [6] reveals the threat of static electromagnetic field on Hall current sensors. The distinctions between Hallspoofing and our work are as follows: ① Hallspoofing is limited to manipulating Hall current sensors, whereas our work addresses the threat of EMI on both Hall and non-Hall sensors. Notably, non-Hall sensors in inverters may render Hallspoofing impractical for precise manipulations. ② Due to the constraints of the magnetic field, the attack distance of Hallspoofing is restricted to a few centimeters. ③ In contrast to Hallspoofing, our analysis is comprehensive, delving into vulnerabilities within the inverter's control algorithms. ④ We revealed a previously unrecognized threat that can directly result in irreversible physical damage to the inverter. Note that achieving `Damage` involves targeting the DC bus voltage sensor, which is distinct from Hall current sensors.

E. Simulation of Shielding Thickness

In the simulation, we set up a dipole antenna as the EMI transmitting source at a distance of 10 mm from the metal casing, with a signal amplitude of 1 V and a frequency of 1000 MHz, and we measured the EMI shielding effectiveness of four kinds of metals.

The result is shown in Fig. 35. As we can see: ① in ideal conditions, the 2 mm thickness of various metals can meet the electromagnetic shielding requirements of the military and aviation field; ② higher thickness can achieve better shielding effect; ③ alloy metal shielding effectiveness is higher than pure metal, which is also often used in engineering. Therefore, under the assumption that the inverter case has adopted the optimal material solution, we recommend that inverter manufacturers increase the thickness of the case metal after weighing the heat dissipation, weight, and other indicators.