Journal of Electronics and Electrical Engineering
https://ojs.wiserpub.com/index.php/JEEE

Research Article

A Self-Adaptive Switching Resilient Control Strategy for Microgrids Under Dynamic False Data Injection Attacks

Chenming Liu[1], Guangting Huang[2], Zhijun Zhang[3], Xiaowu Lin[1], Qicheng Xu[1], Yinghao Shan[1*]

[1] College of Information Science and Technology, Donghua University, Shanghai 201620, China
[2] Xinjiang Zhongjuyuan Power Service Co., Ltd., Urumqi 830009, China
[3] Shanghai Electric Digital Technology Co., Ltd, Shanghai 201101, China

E-mail: shanyh@dhu.edu.cn

Received: 16 October 2025; **Revised:** 19 November 2025; **Accepted:** 28 November 2025

Abstract: In Microgrid (MG) hierarchical control, when the secondary control fails, the islanded MG requires an adaptive primary control to address unforeseen situations. This paper proposes a resilient control strategy for MGs based on a Residual Analysis Observer (RAO). First, an RAO is used to monitor the frequency and voltage of the MG. When a False Data Injection (FDI) attack is detected, an adaptive compensation droop coefficient control method is introduced to correct the frequency and voltage deviations. Second, the concept of the adaptive resistive virtual impedance method is presented, which utilizes adaptive virtual impedance to balance the system's power. To address dynamically changing FDI attacks, a Self-Adaptive Switching Resilient Control (SASRC) strategy is then designed to enhance the system's immunity. Finally, the effectiveness of the SASRC strategy is validated through comprehensive scenario simulations.

Keywords: False Data Injection (FDI) attacks, switching approach, resilient control, Microgrid (MG)

Abbreviation

AC	Alternating Current	ACDC	Adaptive Compensation Droop Coefficient
ARVI	Adaptive Resistive Virtual Impedance	CPS	Cyber-Physical System
DC	Direct Current	DG	Distributed Generator
DoS	Denial-of-Service	ESS	Energy Storage System
FDI	False Data Injection	FPGA	Field Programmable Gate Array
MG	Microgrid	PLL	Phase-Locked Loop
PMUs	Phasor Measurement Units	PV	Photovoltaic
RAO	Residual Analysis Observer	SASRC	Self-Adaptive Switching Resilient Control
SCADA	Supervisory Control and Data Acquisition		

DOI: https://doi.org/10.37256/jeee.4220258923

Symbols

ω_i, E_i	Frequency and voltage of DG_i
P_i, Q_i	Active and reactive power of DG_i
$\delta\omega, \delta E$	Secondary control compensation terms
$\Delta\omega_s$	Synchronization term
ω^*_{MG}, E^*_{MG}	Reference frequency and voltage of the microgrid
i_o	Inverter output current
$y_{fi}(t), y_{Ei}(t)$	Output frequency and voltage of the ith inverter at time t
$e_\xi(t), e_\eta(t)$	Frequency and voltage attack at time t
a_{ij}	Communication status between nodes i and j
$\omega_{ref,u}, \omega_{ref,l}$	Upper and lower limits of reference frequency
ω_{ref}, v_{ref}	Reference frequency and voltage
m_f, n_f	ACDC compensation coefficients
a_{mj}, a_{nj}	Control gains
η_i	Neighbor set of DG_i
u_{dref}, u_{qref}	Output voltages in dq coordinate system
i_{od}, i_{oq}	Output currents in dq coordinate system
$c_{z\omega}, c_{zE}$	Control gains
J_ω, J_v	Judging signals for different events
ξ, η	Segmentation points for frequency and voltage attacks
$\eta_{ref,l}, \eta_{ref^-}, \eta_{ref^+1}, \eta_{ref^+2}, \eta_{ref,u}$	Voltage segmentation points
ω^*_i, E^*_i	Reference frequency and voltage of DG_i
m_{pi}, n_{qi}	Droop coefficients of DG_i
$k_{p\omega}, k_{i\omega}, k_{PE}, k_{iE}$	Secondary control coefficients
ω_{MG}, E_{MG}	Measured frequency and voltage of the microgrid
u_{ref}, u^*_{ref}	Inverter output voltage and its reference
Z_v	Virtual impedance
z_f, z_E	Rated frequency and voltage
$S_{\omega i}, S_{vi}$	RAO output signals for frequency and voltage
b_i	Connection weight
$v_{ref,u}, v_{ref,l}$	Upper and lower limits of reference voltage
γ_ω, γ_v	FDI detection signals for frequency and voltage
P_{ave}, Q_{ave}	Average active and reactive power of DGs
k_{mj}, k_{nj}	Droop coefficient gains of the jth DG
R_v	Adaptive resistive virtual impedance
u^*_{dref}, u^*_{qref}	Reference voltages in dq coordinate system
$R_{v\omega}, R_{vE}$	ARVI for resisting attacks (frequency, voltage)
i_{oabc}	Effective value of output three-phase current
$g_{c\omega}, g_{cv}, g_z$	SASRC event-triggered control gains
$\xi_{ref,l}, \xi_{ref^-}, \xi_{ref^+1}, \xi_{ref^+2}, \xi_{ref,u}$	Frequency segmentation points

1. Introduction

With the development and upgrading of power systems, along with the implementation of global energy conservation and emission reduction initiatives, MGs have gradually become a core technology for industrial transformation, particularly in the efficient generation and utilization of DGs. Through the integration of smart grids and CPSs, users can monitor real-time load conditions and forecast future power load curves using intelligent algorithms. Additionally, they can preconfigure

equipment capacity for energy storage and flexible loads in preparation for adverse weather, thereby preventing power loss due to grid failures. As a typical example of smart grids, MGs have become the focus of research on new power systems [1–3]. As shown in Figure 1, the CPS of an MG primarily consists of a small power generation and distribution system, which includes PV systems, ESSs, thermal and cooling loads, energy conversion devices, monitoring and protection equipment, etc. It is an autonomous system capable of flexibly switching between grid-connected and islanded operations [4].

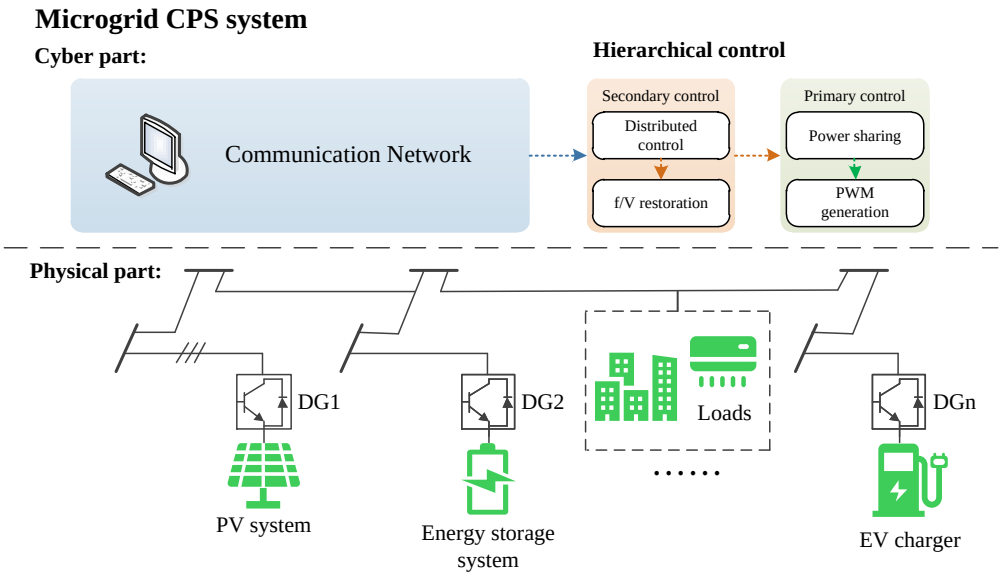

Figure 1. Configuration of the MG-CPS

However, advanced information technologies also introduce potential negative effects to power systems. Numerous studies have highlighted various security risks (such as cyber attacks) in information networks, which can be easily introduced into MGs, leading to failures or paralysis of the power grid system [5, 6]. In [7], cyber attacks targeting transmission networks of power system monitoring and data acquisition systems were reported. It is mentioned in [8, 9] that electric vehicles can easily become a physical port for cyber attacks, which facilitates hackers in carrying out cyber attacks from the load side. In [10], when an MG performs demand-side response with grids, hackers can penetrate the communication layer of the system through the network, thus damaging the local operation of the MG. Therefore, when the system is exposed to cyber attacks, improving the stability of the system is particularly important.

Attackers typically inject small amounts of false data, creating the illusion of normal disturbances in the system to avoid triggering system alerts. Furthermore, the evolving landscape of cyber threats includes sophisticated FDI attacks, such as stealthy attacks designed to bypass conventional bad data detection systems [33] and those targeting critical components like PLLs [31], which can destabilize systems during faults. While these advanced attacks represent critical challenges, this work focuses on a fundamental and direct attack mode against the microgrid's hierarchical control signals. Cyber attacks on MGs may include DoS [11–13] and FDI [14–16] attacks. Among these, FDI attacks are a typical mode, which disrupt decision-making by compromising the data integrity of the power information physical system, successfully bypassing bad data detection mechanisms, and ultimately endangering the security of the power CPSs. Therefore, detecting and mitigating FDI attacks is crucial for the safe and stable operation of MGs. In [17], a tri-level defense model is introduced, specifically designed for large-scale renewable energy power systems, consisting of upper, middle, and lower levels. In [18], a comprehensive protection scheme based on a reduced-order unknown input observer is proposed, providing a centralized fault detection and isolation solution for DC MGs. In [19], an innovative and robust learning-based control framework is presented for wind turbine systems with state constraints. In [20], a new unscented Kalman filter fusion

method is proposed to estimate the state of the system during faults. In [21], a fault detection method for DC MGs based on transient monitoring functions is proposed. While existing FDI detection schemes [17–21] have demonstrated effectiveness in specific contexts, they often overlook the dynamic characteristics of CPSs, particularly the impact of FDI attacks on droop control in microgrids. This limitation motivates our investigation into primary-control-level resilience strategies.

Resilient control is a strategy that enhances the system's resistance and robustness to extreme events. Under resilient control, the system can adapt and recover from such events, minimizing their impact[22–24]. The MG-CPS is a highly nonlinear and complex system. From the physical controllers at the bottom to the upper system optimization layer, MGs face potential security risks at every level of their control hierarchy. Therefore, designing resilient control strategies for MGs is of paramount importance. In [25], a resilience-oriented defense strategy is proposed, considering the uncertainties of attack scenarios. In [26], a collaborative design for secondary frequency regulation of AC MG systems and a network security solution are presented. The observer-based corrective control for isolated island MGs is implemented, enabling collaborative mitigation for AC MG systems. In [27], a resilience-oriented planning strategy for cyber-physical active distribution networks under malicious attacks is proposed. In [28], a distributed resilient controller is designed, based on iterative mean estimation information, to mitigate the effects of cyber attacks in the secondary control. However, the resilient controls in [25–28] are all focused on secondary control. For excessive FDI attacks, or those that penetrate into the primary control, secondary control resilience becomes ineffective, necessitating the disconnection of secondary control. In contrast to prior works [25–28] which primarily focus on securing secondary control, this paper addresses the critical gap of FDI attacks penetrating into the primary control layer. The novelty of this work lies in its primary-control-level resilience strategy, encompassing the ACDC method, the ARVI method, and the overarching SASRC strategy, which together provide a comprehensive defense mechanism for islanded microgrids.

To summarize, the event-triggering mechanism for FDI attack detection in MG-CPS requires further investigation. In addition to solely focusing on isolating FDI attacks, it is also crucial for primary control to provide corresponding compensation to ensure resilient control. Therefore, this paper addresses these issues. From the perspective of MG isolation and restoration, the main contributions are as follows:

(1) When the system cuts off the secondary control by the detection of RAO, an ACDC method has been proposed, which can be used to offset the FDI attack on the primary control after the secondary fall off.

(2) Based on adaptive virtual impedance for the primary control, an ARVI method has been proposed, which can be used to mitigate FDI attacks and achieve the effect of consistent power allocation.

(3) Based on ACDC method and ARVI methods, an SASRC strategy has been proposed, which dynamically selects the optimal control approach to address evolving FDI attacks.

The remainder of this paper is organized as follows. Section 2 provides an overview of the microgrid system and models the FDI attack. Section 3 elaborates on the proposed resilient control strategy, including the ACDC method, the ARVI method, and the integrated SASRC strategy. Section 4 presents comprehensive simulation and hardware-in-the-loop results to validate the effectiveness of the proposed methods. Finally, Section 5 concludes the paper and discusses future work.

2. System overview

As mentioned above, FDI attacks are mainly targeted MG hierarchical control. This section first introduces the structure of droop control, focusing on primary and secondary control. Then, the operational status of the droop control model for MGs under FDI attacks is provided. Finally, we propose a RAO module to detect FDI attack.

2.1 *Microgrid model*

2.1.1 *Droop control*

Adopting the conventional droop control mechanism [29], the relationship between frequency/voltage and active/reactive power is governed by:

$$\begin{cases} \omega_{\mathrm{i}} = \omega^{*}{}_{\mathrm{i}} - m_{\mathrm{pi}} P_{\mathrm{i}} \\ E_{\mathrm{i}} = E^{*}{}_{\mathrm{i}} - n_{\mathrm{qi}} Q_{\mathrm{i}} \end{cases} \tag{1}$$

In order to compensate for the deviation of frequency and voltage, secondary control is added to ensure the stability of frequency and voltage when the load changes and the inverter switching process. Figure 2 is the overall control diagram of the system, which can be divided into primary control part and secondary control part. The main part of the primary control is droop control, which is based on measuring the output voltage and current of the inverter to calculate the active power and reactive power and provides the basis for droop control and virtual impedance module. The secondary control use an external controller to store the deviation from the primary control. At the same time, in order to make multiple inverters connected to form a MG, the frequency and voltage of the MG need to be measured and set as a consistent reference value for secondary control.

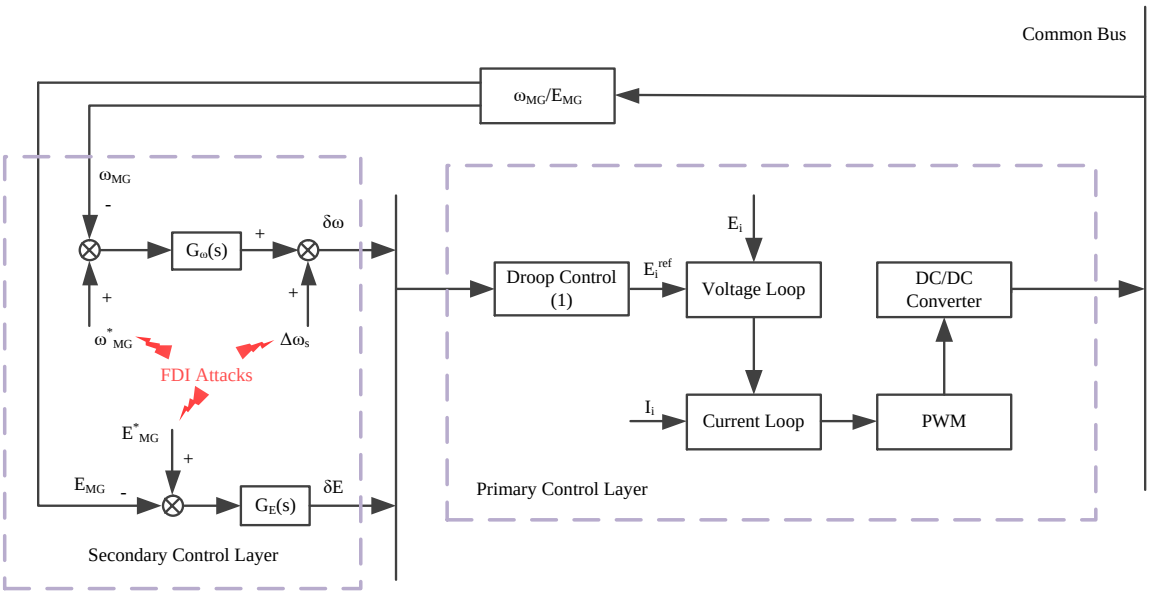

Figure 2. Secondary controllers and FDI attack

The quadratic control in Figure 2, whose control expression can be written as:

$$\delta\omega = k_{p\omega}(\omega^{*}{}_{MG} - \omega_{MG}) + k_{i\omega}\int(\omega^{*}{}_{MG} - \omega_{MG})dt + \Delta\omega_{s} \tag{2}$$

$$\delta \mathrm{E} = k_{PE}(E^{*}{}_{MG} - E_{MG}) + k_{iE}\int(E^{*}{}_{MG} - E_{MG})dt \tag{3}$$

The secondary control compensates for deviations as detailed in [30], while the virtual impedance loop enhances power sharing without additional hardware.

2.1.2 *Virtual impedance*

For various situations of the system, starting from the hardware side can achieve optimization effects, but it will increase costs and may introduce coupling between lines. Overly redundant circuit structures will greatly increase computational difficulty. Therefore, the virtual impedance loop is often introduced which is more flexible and easy to control than the series inductance components, while does not require adding additional hardware equipment. This method does not actually increase the impedance in the control system of the inverter, but multiplies the output current of the inverter with a virtual impedance value as a control signal and adds it to the inverter control loop to achieve the same effect as increasing the actual impedance. Therefore, it is called the virtual impedance method.

For the three-phase inverter with droop control, a virtual impedance control loop is generally added between the droop power and the voltage-current control loop, as shown below:

$$u_{ref} = u^*_{ref} - i_o Z_v \tag{4}$$

The virtual impedance control method is highly flexible, allowing its value to be set as needed. This paper adopts the virtual impedance compensation method to compensate for the original total output impedance of the system.

2.2 *Fault in microgrids*

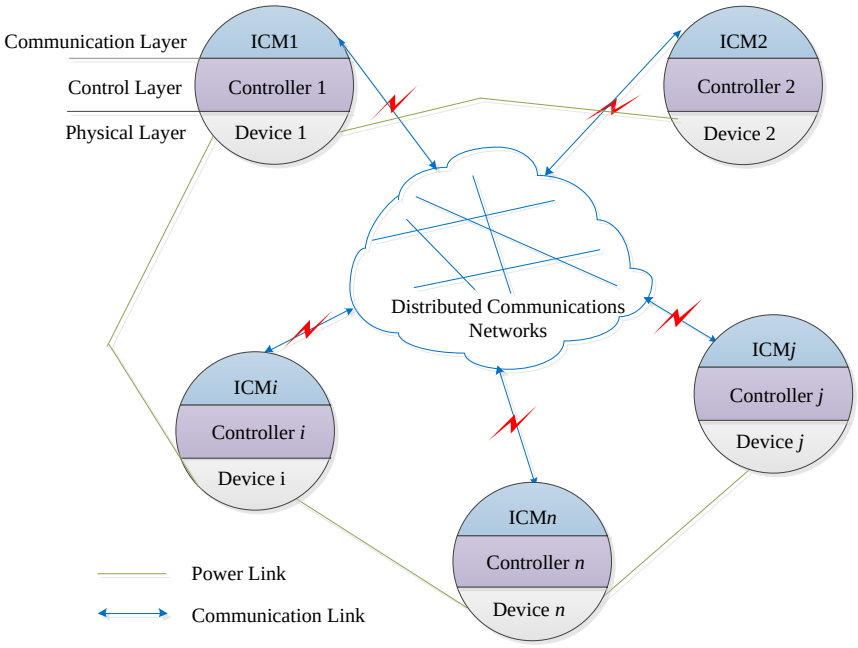

Figure 3. Distributed droop control diagram

Because of the introduction of secondary control that the system is more vulnerable to attacks. As shown in Figure 2, common FDI attacks are added at the secondary frequency compensation, leading the system to out of control. In fact, once inside the control system, an attacker can inject false data in any form. In addition, an attacker can compromise a control system by injecting false data at any weak location, namely actuators, sensors, and communication links. The status of the false data injection attack is as follows:

$$\begin{cases} y_{fi}(t) = z_f - m_i P_i(t) + e_\xi(t) \\ y_{Ei}(t) = z_E - n_i Q_i(t) + e_\eta(t) \end{cases} \tag{5}$$

The main objects of this paper are centralized droop control and distributed droop control. For centralized droop control, FDI attacks will spread evenly to each distributed power source. For distributed droop control, as shown in Figure 3, if DG2 is attacked, subsequent distributed power supplies will be affected. Therefore, if the system continues to operate for a long time under the FDI attacks, it is likely to penetrate in the primary control, resulting in islanded MG paralysis.

2.3 *FDI attack detection*

Since FDI attacks will cause obvious system state anomalies, a RAO is set for each DG using the following formula to detect whether the system is attacked by FDI:

$$S_{\omega i} = \begin{cases} \sum_{j=1}^{N} a_{ij}(\omega_i - \omega_j) + a_{i(N+1)}(\omega_i - \omega_{ref,u}) + a_{i(N+2)}(\omega_i - \omega_{ref,l}) + \\ b_i(\omega_i - \omega_{ref}), i = 1, ..., N \\ 0, i = N+1, N+2 \end{cases} \tag{6}$$

$$S_{vi} = \begin{cases} \sum_{j=1}^{N} a_{ij}(v_i - v_j) + a_{i(N+1)}(v_i - v_{ref,u}) + a_{i(N+2)}(v_i - v_{ref,l}) + \\ b_i(v_i - v_{ref}), i = 1, ..., N \\ 0, i = N+1, N+2 \end{cases} \tag{7}$$

$$\gamma_\omega = \frac{\omega_{ref} - S_{\omega i}}{\omega_{ref}} \tag{8}$$

$$\gamma_v = \frac{v_{ref} - S_{vi}}{v_{ref}} \tag{9}$$

If there is no attack, γ_ω, $\gamma_v = 1$, otherwise γ_ω, $\gamma_v \neq 1$. When a DG is attacked by FDI, due to the centralized control, the attack will spread throughout the network, which seriously affects the stability of the system. Similarly, since the control center of distributed control cannot communicate directly with all DGs, FDI attacks cannot be identified and eliminated by direct access to global information. Therefore, when the secondary control is faced with FDI attacks that traditional methods cannot solve it, it should be cut off in time for islanded MG recovery.

It is important to note that the proposed RAO functions as a local detection mechanism based on consensus principles and pre-defined thresholds. This approach is distinct from, and complementary to, detection methods that rely on system-wide state estimation using synchronized measurements from devices like PMUs or micro-PMUs [32]. The integration of such wide-area monitoring data to enhance detection robustness against stealthier attacks is a promising direction for future work.

3. Resilient control strategy

Facing FDI attacks in the secondary control of MG, the general defense methods include event-triggered mechanism, switching approach and adaptive control, etc. In order to cut out the cyber attacks on secondary control, secondary control shedding can be actively carried out. For the system, it is equivalent to zero the frequency or voltage compensation of the original secondary control, but in the physical connection, the port still exists, so that the system is still at risk of further penetration attack under the primary control operation. For this situation, an event-triggered resilient control scheme is proposed to eliminate this effect and improve the system's immunity to these accidents.

3.1 *Adaptive compensation droop coefficient*

To counteract FDI attacks penetrating into the primary control layer—a scenario rarely addressed in prior works—we propose an ACDC method. The compensated droop control is formulated as:

$$\begin{cases} y_{fi}(t) = z_f - m_f m_i P_i(t) + e_\xi(t) \\ y_{Ei}(t) = z_E - n_f n_i Q_i(t) + e_\eta(t) \end{cases} \tag{10}$$

$$\begin{cases} m_f = \sum\limits_{j\in\eta_i} k_{mj} e_\xi(t)/(m_j P_{ave}) \\ n_f = \sum\limits_{j\in\eta_i} k_{nj} e_\eta(t)/(n_j Q_{ave}) \end{cases} \tag{11}$$

$$\begin{cases} P_{ave} = \sum\limits_{j\in\eta_i} a_{mj}(y_{fj}(t) - z_{fj}) \\ Q_{ave} = \sum\limits_{j\in\eta_i} a_{nj}(y_{Ej}(t) - z_{Ej}) \end{cases} \tag{12}$$

where the adaptive coefficients m_f and n_f are dynamically updated based on local power measurements and attack estimates, enabling real-time compensation without secondary control support.

In order to illustrate the structure better, an overall control diagram of the proposed ACDC method is shown in Figure 4. The specific steps are as follows: first, the frequency or voltage change of the system is detected. According to (8) and (9), when the judgment signal determines that the system is attacked by FDI, P_{ave} or Q_{ave} is obtained through (12), then through (11), m_f or n_f is obtained. Otherwise, the output compensation coefficient is 1. Finally m_f or n_f is added to the frequency or voltage control module of the primary control. This method basically realizes the elimination of FDI, can accurately identify the attack variables of FDI, and resist FDI attacks through closed-loop control.

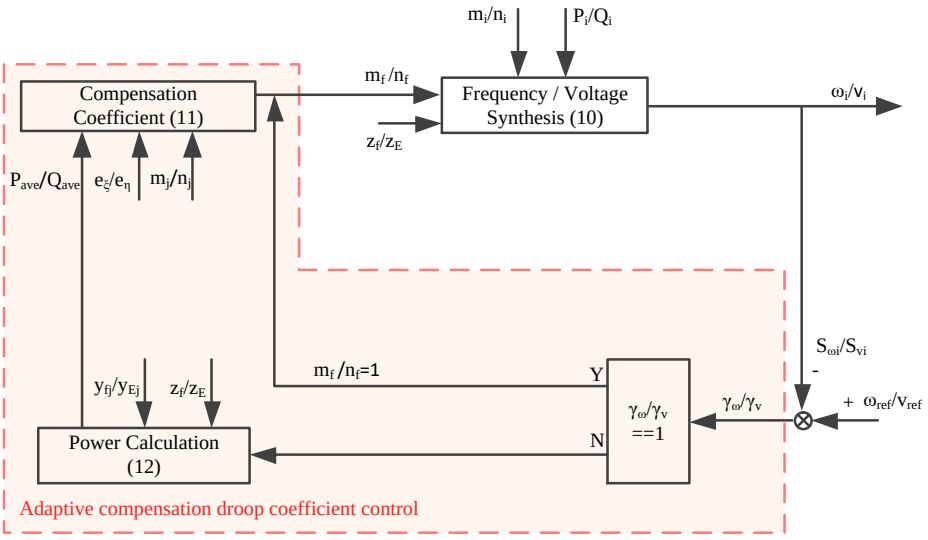

Figure 4. Overall structure of adaptive compensation droop coefficient

3.2 *Adaptive resistive virtual impedance*

After research, it is found that there is reactive power mismatch among DGs. In order to eliminate this effect, adaptive virtual impedance method is generally adopted. According to (4), when virtual impedance Z_v is introduced, it will cause changes in P_i and Q_i of the system, at the same time, it will cause changes in ω_i and E_i due to (1). By calculating the reactive power difference among DGs, the induced reactance difference of each DG can be obtained to compensate the power.

In the voltage compensation loop, if the inductive virtual impedance is introduced, the coupling of the adaptive virtual impedance loop will be caused, which greatly increases the complexity of the system and is not conducive to the subsequent design and calculation. Due to the characteristics of adaptive virtual impedance method, different DG reactive power can be compensated to the same value, so after adding ARVI, DGs can also be adaptive power compensation, achieving the effect of raising frequency and voltage. The formula for the ARVI is as follows:

$$\begin{cases} u_{dref} = u^*_{dref} - i_{od}R_v \\ u_{qref} = u^*_{qref} - i_{oq}R_v \end{cases} \tag{13}$$

$$\begin{cases} R_{v\omega} = \dfrac{e_\xi}{c_{z\omega} i^2_{oabc} m_i} \\ R_{vE} = \dfrac{e_\eta}{c_{zE} i^2_{oabc} n_i} \end{cases} \tag{14}$$

Due to the characteristics of ARVI, a sole compensation frequency/voltage attack will cause an increase in voltage/frequency at the same time. Therefore, if the effect of a sole compensation frequency/voltage is to be achieved, this paper combines the adaptive compensation droop coefficient module to eliminate it.

In order to illustrate the control structure more intuitively, the overall control diagram of the proposed ARVI method is drawn in Figure 5. The specific steps are as follows: first, the frequency or voltage change of the system is detected.

According to (8) and (9), when the judgment signal determines that the system is attacked by FDI, $R_{v\omega}$ and R_{vE} are obtained through (14), otherwise, the output resistive virtual impedance is 0. Finally, the ARVI is added to the voltage synthesis. As mentioned above, if only the frequency or voltage is needed to be compensated, then the frequency or voltage compensation of the ARVI can be obtained by calculating the module, converted into the voltage or frequency change, and substituted into the ACDC module (10) to achieve the effect of compensating only the frequency or voltage.

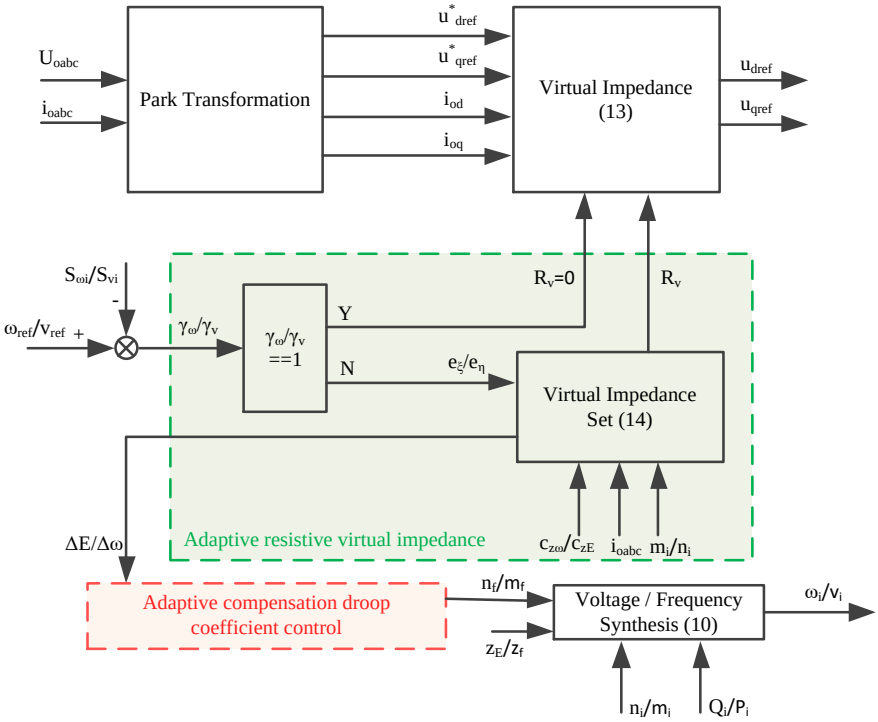

Figure 5. Overall structure of adaptive resistive virtual impedance

3.3 *Self-adaptive switching resilient control*

Although the ACDC and ARVI method proposed above can effectively resist FDI attacks, they have their own limitations. When the amount of attack is tiny, the effect of using ARVI method is the most direct and effective, and the effect of power distribution can be achieved, but the ARVI method can only achieve the increase of frequency and voltage, and for the excessive amount of attack, it is necessary to use the ACDC method to switch control. Therefore, an SASRC strategy is proposed to classify the detected signals and adjust them with different control strategies.

$$J_\omega = \begin{cases} g_{c\omega}=1, g_{cv}=0, g_z=0 : if\, \gamma_\omega \subset \left[\xi_{ref,l}, \xi_{ref^-}\right) \\ g_{c\omega}=0, g_{cv}=1, g_z=1 : if\, \gamma_\omega \subset \left[\xi_{ref^-}, 1\right) \\ g_{c\omega}=1, g_{cv}=1, g_z=1 : if\, \gamma_\omega \subset \left(1, \xi_{ref^+1}\right] \\ g_{c\omega}=0, g_{cv}=1, g_z=1 : if\, \gamma_\omega \subset \left(\xi_{ref^+1}, \xi_{ref^+2}\right] \\ g_{c\omega}=1, g_{cv}=0, g_z=0 : if\, \gamma_\omega \subset \left(\xi_{ref^+2}, \xi_{ref,u}\right] \end{cases} \tag{15}$$

$$J_v = \begin{cases} g_{c\omega} = 0, g_{cv} = 1, g_z = 0 : if \gamma_v \subset \left[\eta_{ref,l}, \eta_{ref^-}\right) \\ g_{c\omega} = 1, g_{cv} = 0, g_z = 1 : if \gamma_v \subset \left[\eta_{ref^-}, 1\right) \\ g_{c\omega} = 1, g_{cv} = 1, g_z = 1 : if \gamma_v \subset \left(1, \eta_{ref^+1}\right] \\ g_{c\omega} = 1, g_{cv} = 0, g_z = 1 : if \gamma_v \subset \left(\eta_{ref^+1}, \eta_{ref^+2}\right] \\ g_{c\omega} = 0, g_{cv} = 1, g_z = 0 : if \gamma_v \subset \left(\eta_{ref^+2}, \eta_{ref,u}\right] \end{cases} \tag{16}$$

Once the condition of event-triggered is met, the system sends the event-triggered control gain to the corresponding unit through the loop to realize the self-adaptive switching of the system against different FDI attacks. When the attack signal is positive, FDI attacks can be used to restore the system to achieve the effect of secondary control. When the attack signal is negative, the switching control can restore the frequency and voltage to the stable value of primary control to resist FDI attacks.

4. Simulation validation

The proposed control methods and strategy are evaluated on a typical islanded AC microgrid test system. The system consists of four DGs connected through transmission lines to common loads. Each DG is interfaced via a three-phase voltage source inverter with LC filters. The system operates in islanded mode with hierarchical control structure, including primary droop control and secondary control for voltage and frequency restoration. The communication network follows a distributed topology for secondary control coordination. To evaluate the performance of the proposed overall control methods and strategy, this section presents a comprehensive study of these two methods (ACDC, ARVI) and one strategy (SASRC). The detailed system settings and parameters are provided in Tables 1 and 2. The simulation model and control algorithm are implemented in MATLAB/Simulink on a desktop computer with an i5-13490F CPU and 64GB memory.

Table 1. System configuration and inverter parameters

Parameter Name	Symbol	Value
DC-link voltage	V_{dc}	0.8 kV
System rated voltage	V_{rated}	380 V
System rated frequency	f_{rated}	50 Hz
Sampling frequency	f_s	20 kHz
Control interval	T_s	5 μs
Filter inductance	L_f	0.6 mH
Filter capacitance	C_f	1500 μF
Filter parasitic resistance	R_f	0.01 Ω
Switching frequency	f_{sw}	10 kHz
DG1 line impedance	Z_{line1}	0.1 + j0.754 Ω
DG2 line impedance	Z_{line2}	0.1 + j0.754 Ω
DG3 line impedance	Z_{line3}	0.12 + j0.8 Ω
DG4 line impedance	Z_{line4}	0.12 + j0.8 Ω
Local load (each DG)	P_{local}	5 kW
Common load	P_{common}	20 kW

Table 2. Control parameters

Parameter Name	Symbol	Value
Frequency droop coefficient	m_{pi}	1.0×10^{-4} Hz/W
Voltage droop coefficient	n_{qi}	1.0×10^{-3} V/Var
Frequency proportional gain	$k_{p\omega}$	0.5
Frequency integral gain	$k_{i\omega}$	10
Voltage proportional gain	k_{PE}	0.5
Voltage integral gain	k_{IE}	10
Active power control gain	a_{mj}	−50000
Reactive power control gain	a_{nj}	−15000
Droop coefficient gain (active)	k_{mj}	2.5
Droop coefficient gain (reactive)	k_{nj}	3.5
Frequency compensation gain	$c_{z\omega}$	0.04
Voltage compensation gain	c_{zE}	1.2
Output current reference	i_{oabc}	30.88 A
Lower limit	$\xi_{ref,l}$	0.997
Lower threshold	ξ_{ref^-}	0.9989
Upper threshold 1	ξ_{ref^+1}	1.0004
Upper threshold 2	ξ_{ref^+2}	1.001
Upper limit	$\xi_{ref,u}$	1.005
Lower limit	$\eta_{ref,l}$	0.995
Lower threshold	η_{ref^-}	0.998
Upper threshold 1	η_{ref^+1}	1.002
Upper threshold 2	η_{ref^+2}	1.005
Upper limit	$\eta_{ref,u}$	1.014

4.1 *Simulation of two DGs under FDI attacks*

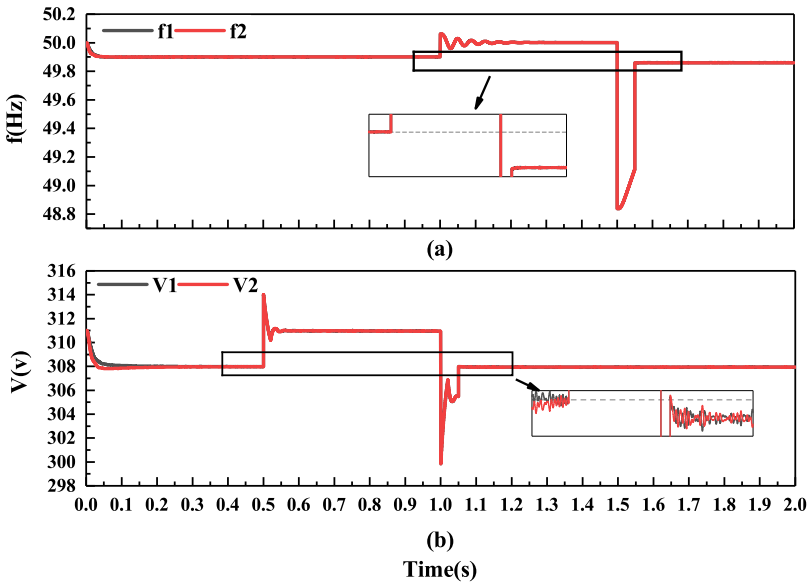

Figure 6. Complete operating status diagram of the system

To better explain the situation of FDI attacks, the frequency operation state of the system is shown in Figure 6a. From 0 to 1 s, the system is under primary droop control operation, and it is verified that (1) will cause a decrease in frequency; 1 to 1.5 s is the secondary control operation, it can be seen that the frequency compensation to 50Hz and stable operation. At 1.5 s the system suffers from FDI attack, the system detected the frequency anomaly, and timely cut off the secondary control. While suffering from penetration attack during the cut off, set the cut off signal as a constant, and eventually led to the frequency anomaly under the first control. The voltage running state of the system is shown in Figure 6b. From 0 to 0.5 s, the system is under primary droop control operation, and then 0.5 to 1 s is switched to a secondary control operation. It can be seen that the voltage compensation to 311V and stable operation. The system was attacked by FDI at 1 s, and the voltage anomaly was detected and the secondary control was cut off in time. However, the data was modified during the cut off, and the cut-off signal was set to a non-zero constant, resulting in the voltage anomaly under the primary control. The subsequent simulation experiments will focus on the verification of a control penetration attack.

4.2 *Simulation of two proposed methods under constant FDI attacks*

For the constant FDI attacks, this section will verify two different adaptive methods (ADCD, ARVI) mentioned above, respectively setting the FDI attacks as positive and negative constant, adding them to the position of frequency or voltage droop synthesis, and using the proposed methods (ADCD, ARVI) to carry out adaptive cancellation.

4.2.1 *Simulation of adaptive compensation droop coefficient control*

FDI attacks are injected into frequency and voltage respectively to verify the feasibility of this method. First, as shown in Figure 7 is the verification of frequency attack. The initial state after the attack is compared with the operating state with the ACDC method added. $f_{fdi}1$ and $f_{fdi}2$ are the frequencies of DG_1 and DG_2 under FDI attack state, and f_c1 and f_c2 are the frequencies of DG_1 and DG_2 after the ACDC method is added. Figure 7a set negative constant attack verifies that the ACDC method compensates the frequency to the stable value of primary control. The positive constant attack set in Figure 7b,c verifies that the ACDC method can compensate the system to stable value of secondary control by using the positive constant attack.

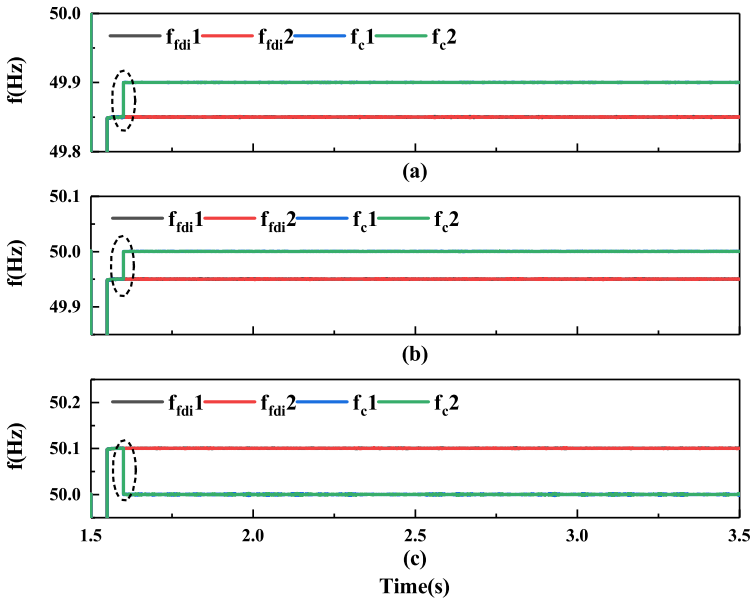

Figure 7. Simulation of frequency adaptive compensation droop coefficient

Then comes the verification of voltage attack. As shown in Figure 8, the initial state after attack is compared with the operating state with the ACDC method added. $V_{fdi}1$ and $V_{fdi}2$ are the voltages of DG_1 and DG_2 under FDI attack, and V_c1 and V_c2 are the voltages of DG_1 and DG_2 after the ACDC method is added. Figure 8a sets the negative constant attack, which verifies that the ACDC method compensates the voltage to the stable value of the primary control. The positive constant attack set in Figure 8b,c verifies that the ACDC method can use the positive constant attack to compensate the voltage to the stable value of the secondary control.

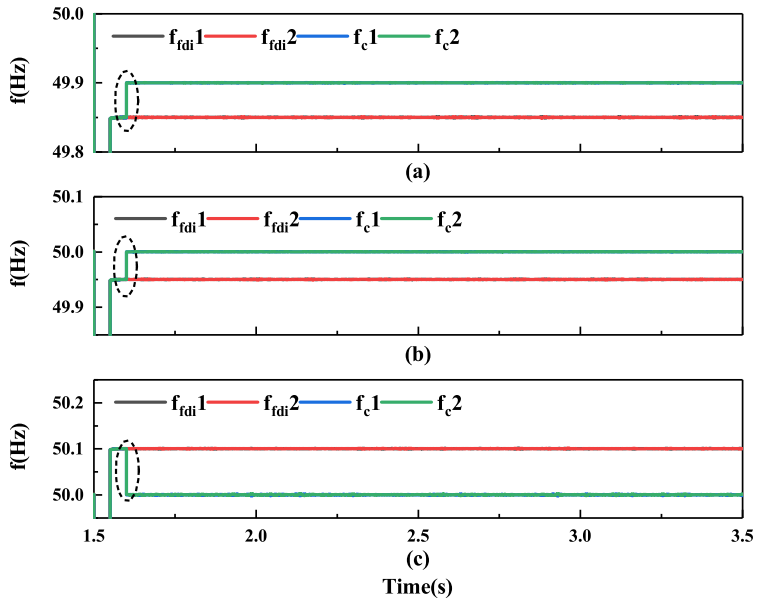

Figure 8. Simulation of voltage adaptive compensation droop coefficient

4.2.2 *Simulation of adaptive resistive virtual impedance*

First, the operating state when the voltage is subjected to FDI attacks is simulated, as shown in Figure 9b. After injecting negative constant attack at 1.5s, the system uses the ARVI to restore the voltage to the primary state stable value at 1.6s. $V_{Rv}1$ and $V_{Rv}2$ are the voltages of DG_1 and DG_2 after the ARVI method is added. As shown in Figure 9a, due to the characteristics of the ARVI method, the frequency rises synchronously. $f_{Rv}1$ and $f_{Rv}2$ are the frequencies of DG_1 and DG_2 after the ARVI is added. After adding the ACDC method, the frequency can be compensated to the stable value of the secondary control by using the increment of the ARVI method.

Then, the feasibility of ARVI under positive constant attack is verified. FDI attacks are added to frequency and voltage respectively, as shown in Figure 10a,d. After ARVI method, positive constant attacks can be used to restore the system to the stable value of secondary control. And as shown in Figure 10b,c, the characteristics of voltage and frequency can be changed synchronously by using the positive constant attacks. Voltage and frequency can be compensated to the stable value of secondary control by ACDC method, so as to achieve the effect of secondary control.

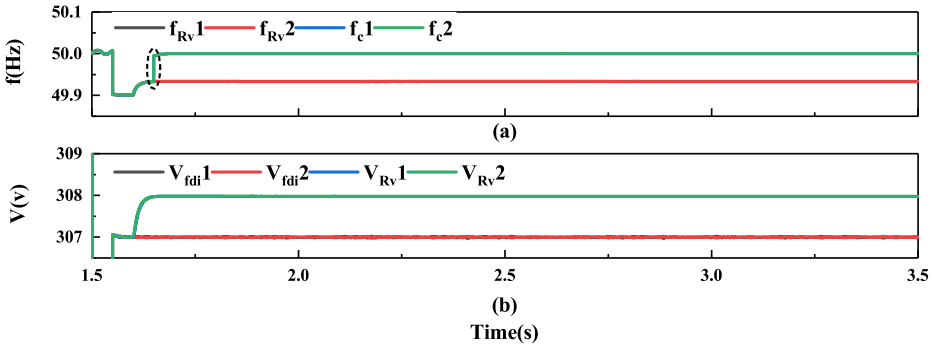

Figure 9. Simulation of adaptive resistive virtual impedance resisting positive constant FDI attack

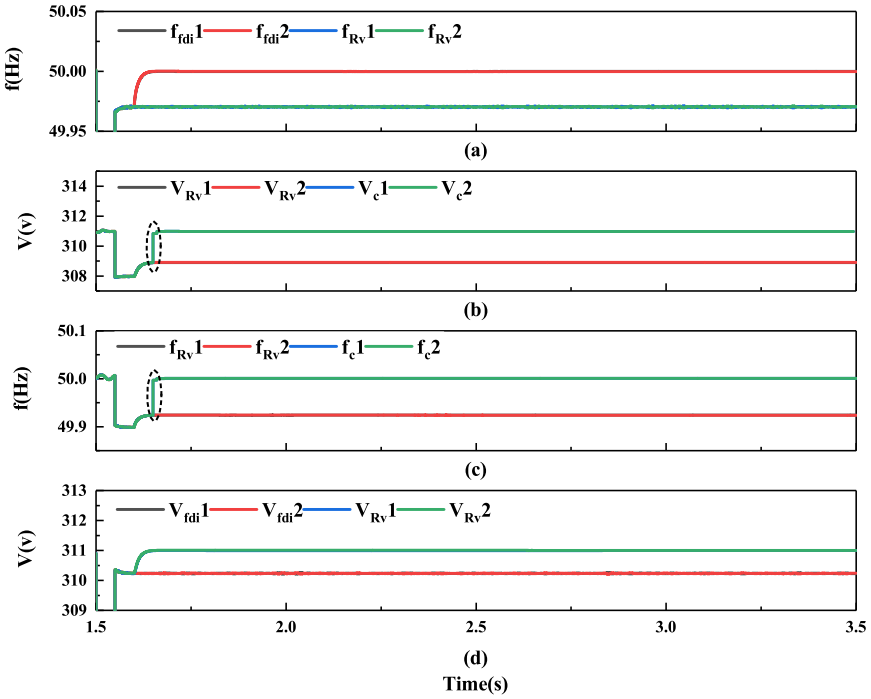

Figure 10. Simulation of adaptive resistive virtual impedance resisting negative constant FDI attack

4.3 *Simulation of the proposed strategy under dynamic FDI attacks*

In this scenario, the SASRC strategy is compared with the traditional method, and sinusoidal attacks are added to 4 DGs to verify the feasibility of proposed SASRC strategy against continuous change attacks. First is the verification of frequency attacks. As shown in Figure 11a, the system frequency is subjected to sinusoidal attacks. As shown in Figure 11b, when the system detects the FDI attacks, the traditional resilient control can restore the frequency to approximately 50Hz. However, as time accumulates, the fluctuation of the frequency gradually becomes larger after 3s, with a maximum deviation of up to ±2 Hz. In contrast, the proposed SASRC strategy, as shown in Figure 11c, can quickly stabilize the frequency at 50Hz with a significantly smaller maximum deviation of less than ±0.02 Hz and a shorter settling time. The local amplification demonstrates the adaptive triggering of the SASRC, which effectively suppresses the oscillations caused by the sinusoidal attack.

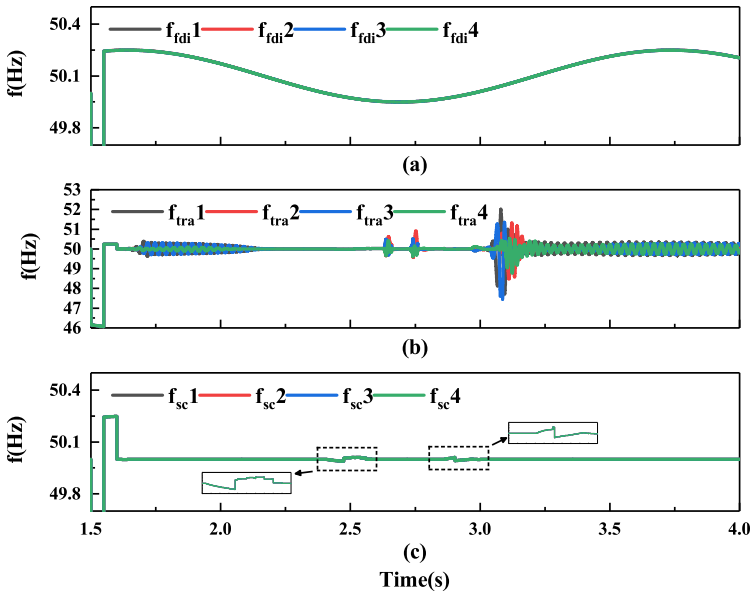

Figure 11. Simulation of sinusoidal FDI attack on frequency

Then comes the verification of voltage attack. As shown in Figure 12a, the system voltage is subjected to sinusoidal attack. As can be seen from Figure 12b, the traditional method eventually restores the voltage to 311 V, but exhibits large initial fluctuations with a peak overshoot of about 5 V. In contrast, the SASRC strategy, as shown in Figure 12c, rapidly stabilizes the voltage to 311 V with a negligible overshoot of less than 1 V, demonstrating a much faster dynamic response and superior stability.

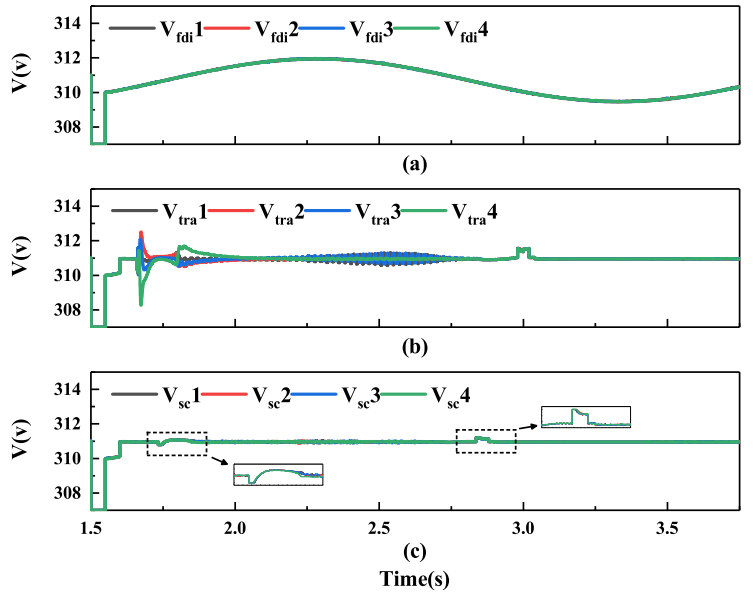

Figure 12. Simulation of sinusoidal FDI attack on voltage

4.4 *FPGA-in-the-loop experiments*

In this study, a hardware-in-the-loop simulation framework is used to verify the performance of the designed SASRC strategy against random step FDI attacks. Hardware-in-the-loop is a semi-physical real-time simulation technique. In this principle, FPGA and MATLAB are combined, and the personal computer is physically connected to the FPGA. In this research, the communication between FPGA and MATLAB is realized by using the joint test action group method.

The experimental principle is shown in Figure 13. First, the Simulink generates and transmits signals to the FPGA. The FPGA then gets the signal and transmits it to Simulink for display. The false data outputted through the "key" on FPGA can be used to simulate FDI attacks in this study, which is transmitted to the computer side of the Simulink model. Finally, the false data is inputted into the MG system for FDI attacks. The experimental results of the proposed method of resisting FDI attacks are shown in the following ways.

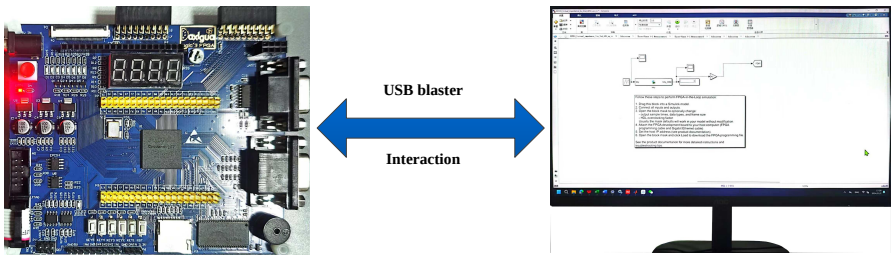

Figure 13. Hardware-in-the-loop experiment structure

Figure 14 shows the comparison of frequency FDI attacks by FPGA under the traditional method and the proposed SASRC strategy, and Figure 14a shows the input value of FDI attacks by FPGA. Due to the distributed consistency characteristic, the system under traditional method can adapt to recover to 50Hz, but large fluctuations will occur, as shown in Figure 14b. However, SASRC can better perform adaptive compensation for step signals, as shown in Figure 14c, and the fluctuation does not exceed 0.025Hz.

Figure 15 shows the comparison of voltage FDI attacks by FPGA under the traditional method and the proposed SASRC strategy, and Figure 15a shows the input value of FDI attacks by FPGA. Same as the state of frequency, the system under traditional method can adapt to recover to 50Hz, but large fluctuations will occur, as shown in Figure 15b. While SASRC strategy can better perform adaptive compensation for step signals, as shown in Figure 15c, and the fluctuation does not exceed 0.01V.

The FPGA-in-the-loop results validate the practical feasibility and real-time performance of the SASRC strategy. The random step attacks represent a severe test scenario with high-frequency, unpredictable changes. This demonstrates that the logic for attack detection, classification, and control switching can be executed within the stringent timing constraints of a real control system. The strategy's ability to handle random steps confirms its robustness against non-smooth, abrupt cyber threats, a critical requirement for real-world deployment.

The comprehensive simulation and HIL results demonstrate that the proposed SASRC strategy provides a multi-layered defense mechanism for islanded microgrids. The ACDC method serves as a precise tool for direct attack compensation, while the ARVI method offers a robust means for voltage support and power sharing. The synergy between them, orchestrated by the SASRC's event-triggered switching logic, creates a system that is more resilient than the sum of its parts. This strategy effectively bridges the gap between primary and secondary control resilience, ensuring system survival even when secondary control is compromised and attacked data penetrates to the primary level.

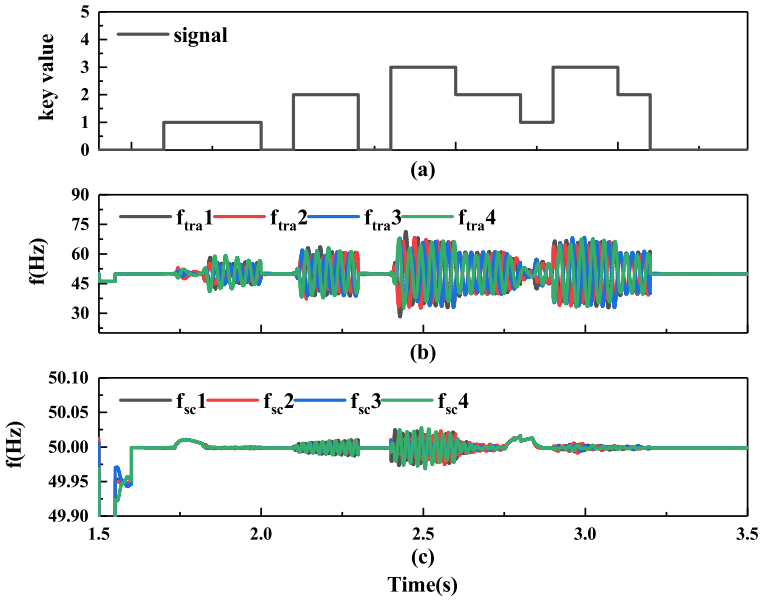

Figure 14. Simulation of frequency comparison between traditional methods and switching control in hardware-in-the-loop

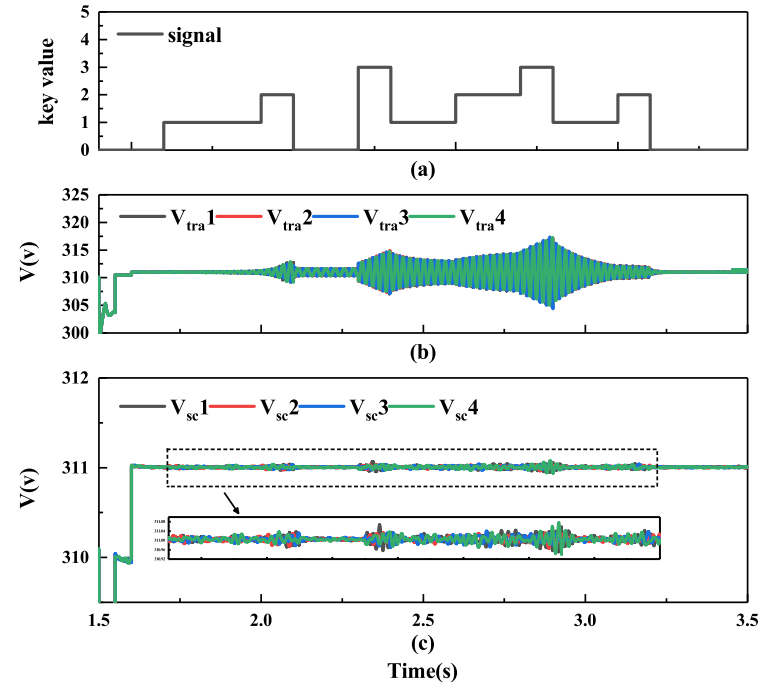

Figure 15. Simulation of voltage comparison between traditional methods and switching control in hardware-in-the-loop

5. Conclusion

In this paper, two adaptive methods and one resilient control strategy are proposed to enhance the resilience of MGs under FDI attacks. First, the ACDC method is proposed to quickly compensate for frequency and voltage, effectively

resisting FDI attacks, as demonstrated by its capability to restore system frequency and voltage to their stable references under constant attacks. Second, the ARVI method is introduced to raise frequency and voltage, ensuring consistent power distribution and providing complementary resilience against attacks that cause power imbalances. Third, by integrating the two adaptive methods, the SASRC strategy is developed to handle abnormal FDI attacks, with simulation and hardware-in-the-loop results validating its superior performance in maintaining frequency within ±0.02 Hz of the nominal value and limiting voltage overshoot to less than 1 V during severe sinusoidal attacks, thereby significantly enhancing the system's immunity and resilience. The comprehensive study confirms that the SASRC strategy outperforms traditional methods in both transient response and steady-state stability under cyber threats. In future work, research will focus on countering combined cyber threats. Additionally, we plan to extend the proposed strategy to defend against a broader class of sophisticated cyber-physical threats. This includes enhancing detection for stealthy FDI attacks, developing mitigation techniques for attacks targeting grid-synchronization units like PLLs, and integrating our control-centric approach with data-driven monitoring frameworks that utilize advanced sensors.

Conflicts of interest

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

[1] B. Sharif, E. R. Sanseverino, V. Di Dio, and M. Beccali, "Enhancing frequency management in renewable-powered smart grids with metaheuristic optimization of cascaded controller," *Computers and Electrical Engineering*, vol. 129, p. 110839, 2026.

[2] J. Hu, H. Zhang, H. Liu, and X. Yu, "A survey on sliding mode control for networked control systems," *International Journal of Systems Science*, vol. 52, no. 6, pp. 1129-1147, 2021.

[3] D. Ding, Q.-L. Han, X. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: a survey," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 176-190, 2020.

[4] T. M. Ghazal, M. K. Hasan, U. A. Mokhtar, N. Safie, A. Alshamayleh, and M. Ahmad, "Machine learning-based real-time outage fault detection for distribution networks in smart grid," *Energy Reports*, vol. 14, pp. 3739-3752, 2025.

[5] M. Chlela, D. Mascarella, G. Joos, and M. Kassouf, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4702-4711, 2017.

[6] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power system risk assessment in cyber attacks considering the role of protection systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 572-580, 2016.

[7] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318, 2016.

[8] M. R. Khalghani, J. Solanki, S. K. Solanki, M. H. Khooban, and A. Sargolzaei, "Resilient frequency control design for microgrids under false data injection," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 3, pp. 2151-2162, 2020.

[9] E. Tian, Z. Wu, and X. Xie, "Codesign of FDI attacks detection, isolation, and mitigation for complex microgrid systems: an HBF-NN-based approach," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 5, pp. 6156-6165, 2022.

[10] H. Zhang, D. Yue, C. Dou, and G. P. Hancke, "Resilient optimal defensive strategy of micro-grids system via distributed deep reinforcement learning approach against FDI attack," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 1, pp. 598-608, 2022.

[11] X.-K. Liu, C. Wen, Q. Xu, and Y.-W. Wang, "Resilient control and analysis for DC microgrid system under DoS and impulsive FDI attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 3742-3754, 2021.

[12] X.-K. Liu, S.-Q. Wang, M. Chi, Z.-W. Liu, and Y.-W. Wang, "Resilient secondary control and stability analysis for DC microgrids under mixed cyber attacks," *IEEE Transactions on Industrial Electronics*, vol. 71, no. 2, pp. 1938-1947, 2023.
[13] Y. Xia, Y. Xu, S. Mondal, and A. K. Gupta, "A transfer learning-based method for cyber-attack tolerance in distributed control of microgrids," *IEEE Transactions on Smart Grid*, vol. 15, no. 2, pp. 1234-1245, 2023.
[14] A. J. Abianeh, Y. Wan, F. Ferdowsi, N. Mijatovic, and T. Dragičević, "Vulnerability identification and remediation of FDI attacks in islanded DC microgrids using multiagent reinforcement learning," *IEEE Transactions on Power Electronics*, vol. 37, no. 6, pp. 6359-6370, 2021.
[15] M. S. Sadabadi, "A resilient-by-design distributed control framework for cyber-physical DC microgrids," *IEEE Transactions on Control Systems Technology*, vol. 31, no. 6, pp. 2345-2356, 2023.
[16] J. Callenes and M. Poshtan, "Dynamic reconfiguration for resilient state estimation against cyber attacks," *IEEE Transactions on Emerging Topics in Computing*, vol. 11, no. 3, pp. 567-578, 2023.
[17] Z. Zhao, Y. Shang, B. Qi, Y. Wang, Y. Sun, and Q. Zhang, "Research on defense strategies for power system frequency stability under false data injection attacks," *Applied Energy*, vol. 371, p. 123711, 2024.
[18] T. Wang, L. Liang, Z. Hao, A. Monti, and F. Ponci, "A comprehensive fault detection and isolation method for DC microgrids using reduced-order unknown input observers," *IEEE Transactions on Power Delivery*, vol. 39, no. 1, pp. 479-495, 2023.
[19] M. Mazare and H. Ramezani, "Enhancing cybersecurity in wind turbines: a resilient reinforcement learning-based optimal control for mitigating FDI attacks," *Applied Energy*, vol. 373, p. 123939, 2024.
[20] A. Vafamand, B. Moshiri, and N. Vafamand, "Fusing unscented Kalman filter to detect and isolate sensor faults in DC microgrids with CPLs," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1-8, 2021.
[21] M. A. Jarrahi, H. Samet, and T. Ghanbari, "Fault detection in DC microgrid: a transient monitoring function-based method," *IEEE Transactions on Industrial Electronics*, vol. 70, no. 6, pp. 6284-6294, 2022.
[22] Y. Yu, G.-P. Liu, and W. Hu, "Security tracking control for discrete-time stochastic systems subject to cyber attacks," *ISA Transactions*, vol. 127, pp. 133-145, 2022.
[23] J. Xiao, L. Wang, Z. Qin, and P. Bauer, "A resilience enhanced secondary control for AC micro-grids," *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 810-820, 2023.
[24] Y. Du, X. Lu, B. Chen, and F. Lin, "Resiliency augmented hybrid AC and DC distribution systems with inverter-dominated dynamic microgrids," *IEEE Transactions on Smart Grid*, vol. 13, no. 5, pp. 4088-4101, 2022.
[25] X. Kong, Z. Lu, Y. Li, X. Guo, J. Zhang, and S. Ding, "Resilience-oriented defense strategy for power systems against uncertain malicious coordinated attacks," *Applied Energy*, vol. 378, p. 124785, 2025.
[26] T. Huang, D. Wu, and M. Ilić, "Cyber-resilient automatic generation control for systems of AC microgrids," *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 886-898, 2023.
[27] X. Jing, W. Qin, H. Yao, X. Han, and P. Wang, "Resilience-oriented planning strategy for the cyber-physical ADN under malicious attacks," *Applied Energy*, vol. 353, p. 122052, 2024.
[28] H. Yang, C. Deng, X. Xie, and L. Ding, "Distributed resilient secondary control for AC microgrid under FDI attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 70, no. 7, pp. 2570-2574, 2023.
[29] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. De Vicuña, and M. Castilla, "Hierarchical control of droop-controlled AC and DC microgrids—a general approach toward standardization," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 1, pp. 158-172, 2010.
[30] Y. Shan, A. Pan, and H. Liu, "A switching event-triggered resilient control scheme for primary and secondary levels in AC microgrids," *ISA Transactions*, vol. 127, pp. 216-228, 2022.
[31] A. Kontou, M. Syed, A. Paspatis, Z. Feng, C. Konstantinou, and N. Hatziargyriou, "Exploiting the inherent cyber resilience of inverter-dominated microgrids against PLL attack," *IEEE Transactions on Industrial Electronics*, vol. 72, no. 1, pp. 1-6, 2025.
[32] N. P. Theodorakatos, R. Babu, C. A. Theodoridis, and A. P. Moschoudis, "Mathematical models for the single-channel and multi-channel PMU allocation problem and their solution algorithms," *Algorithms*, vol. 17, no. 5, p. 191, 2024.
[33] T. A. Alexopoulos, G. N. Korres, and N. M. Manousakis, "Complementarity reformulations for false data injection attacks on PMU-only state estimation," *Electric Power Systems Research*, vol. 189, p. 106796, 2020.