IEEE Open Journal of
Power Electronics

Received 31 March 2023; revised 22 June 2023; accepted 27 June 2023. Date of publication 29 June 2023;
date of current version 13 July 2023. The review of this article was arranged by Associate Editor Jin Ye.

Digital Object Identifier 10.1109/OJPEL.2023.3290900

Data-Driven Cyberphysical Anomaly Detection for Microgrids With GFM Inverters

XIAORUI LIU (Student Member, IEEE), AND HUI LI (Fellow, IEEE)

Center for Advanced Power Systems, Florida State University, Tallahassee, FL 32310 USA

CORRESPONDING AUTHOR: HUI LI (email: hli@caps.fsu.edu)

ABSTRACT Microgrids (MGs) have gained significant attention considering their enhanced capability to integrate increasing distributed energy resources (DERs). The application of grid forming (GFM) inverters in a MG can control voltage/frequency, enable both islanded and grid-connected operation, and achieve 100% penetration. However, cyberphysical anomaly detection for a MG with GFM inverters has not been investigated before. In this article, the cyberphysical security of an ac MG with multiple GFM inverters is comprehensively assessed by considering short-circuit high-impedance faults (HIFs) as well as firstly exploiting False Data Injection Attacks (FDIAs) against centralized communication networks. Although the applied IEEE 1547-2018 based protection function could detect abnormal conditions, there exist cyberphysical anomalies could bypass it. In order to accomplish the detection and classification of such anomaly cases, a novel LSTM-based approach is proposed to identify the multi-class pattern regarding normal, cyberphysical threats during islanded and grid-connected by utilizing time series point of common coupling (PCC) frequency data as the paramount feature to effectively reflect the system operation status. The simulation is conducted in OPAL-RT real-time environment and the effectiveness of the proposed strategy is verified with an average detection accuracy of 94.72%.

INDEX TERMS Anomaly detection and classification, cyberphysical security, data-driven, FDIAs, GFM inverters, HIFs, real-time simulation.

NOMENCLATURE

MG	Microgrid.
DER	Distributed energy resource.
GFM	Grid forming.
GFL	Grid following.
RES	Renewable energy sources.
LC	Local controller.
MGC	Microgrid controller.
MGCC	Microgrid central controller.
DoS	Denial-of-service.
FDIA	False data injection attack.
ANN	Artificial neural network.
LSTM	Long-short-term-memory.
HIF	High-impedance fault.
PCC	Point of common coupling.
ω, ω^*	Angular frequency and its reference.
V, V^*	Magnitude of inverter output voltage and its reference.
k_P, k_Q	Droop coefficients.
P, Q	Active power and reactive power.
P^*, Q^*	Reference of active and reactive power.
$\Delta\omega$, Δv	Compensated frequency/voltage.
ω_{pcc}, V_{pcc}	Frequency/voltage at PCC.
ω^*_{pcc}, V^*_{pcc}	Frequency/voltage reference at PCC.
θ_{g}, θ_{pcc}	Phase angle of grid/PCC.
$\Delta\omega'$	Compensated frequency in synchronization.
P_{g}, Q_{g}	Active/reactive power injected to grid.
P^*_{g}, Q^*_{g}	Active/reactive power reference.
$k_{P\omega}$, $k_{I\omega}$	PI coefficients of secondary frequency control.
k_{pv}, k_{Iv}	PI coefficients of secondary voltage control.
$k_{P\omega'}$, $k_{I\omega'}$	PI coefficients of synchronization control.
k_{Pgp}, k_{Igp}	PI coefficients of tertiary active power control.
k_{Pgq}, k_{Igq}	PI coefficients of tertiary reactive power control.
OV/UV	Over voltage, under voltage.
OF/UF	Over frequency, under frequency.

1, 2, 3LG	Single, two, three-phase line-to-ground fault.
2, 3LL	Two phase, three phase line-to-line fault.
$\Delta X, \Delta X_a$	Transferred data and altered transferred data.
T_a	Attack duration.
μ, σ^2	Mean and variance of Gaussian distribution
γ_{sca}	Scaling attack factor.
$\gamma_{sin}, \omega_{sin}$	Amplitude and frequency of sinusoidal signal.
γ_c	Change ratio of continuous pulse signal.
D	Duty cycle of continuous pulse signal.
f_t, i_t, o_t, h_t	Forget, input, output, hidden gate.
w_f, w_i, w_o, w_c	Weight matrices
b_f, b_i, b_o, b_c	Bias vectors.
$y, \hat{y}$	Ground truths and predicted class.

I. INTRODUCTION

Microgrids (MGs) facilitate the increasing number of distributed energy resources (DERs) and improve power transfer efficiency by utilizing local energy sources to serve neighboring consumers. In addition, the capability to operate in a self-sufficient mode in case of grid emergencies enhances the resiliency and stability of the regional electric grid. In particular, the grid forming (GFM) inverters operate as AC voltage sources with controllable frequency and voltage. It could function well in either high or low penetration level by using droop laws to control voltage sources [1], [2], [3], [4], [5]. Grid following (GFL) inverters act as current sources to supply adequate active and reactive power to the grid. Due to the intrinsic difference between GFM and GFL control, the dynamic performance of GFM inverters improves while GFL inverters degrade with the increase of penetration level [6]. Furthermore, only GFM inverters can operate in a 100% penetration level system, as a purely inverter-supported system. As a promising role to address the challenges of increased penetration of renewable energy sources (RES) in bulk power systems, it has been broadly accepted that the GFM converters will play a more predominant role in the future electrical grid. Extensive research works on GFM inverters have been conducted during islanded operation [7], [8], [9]. As an extended application of the GFM inverter, hierarchical control is proposed in [10] to be suitable in both islanded and grid-connected operations. More specifically, the primary control loop located in the local controller (LC) leverages the droop control to regulate the frequency and voltage of each inverter. Meanwhile, aiming to compensate for the droop deviations and enable the grid-connected feature, system-level controls including secondary, synchronization, and tertiary control are deployed in the MG controller (MGC).

To enable the information exchange between LC and MGC, a low-bandwidth communication network has to be established. There are two communication configurations, centralized and distributed. The centralized one refers to one-to-many communication between MG central controller (MGCC) and each LC which is standardized for MG control to achieve accurate power sharing [11]. On the contrary, distributed communication is a peer-to-peer method as presented in [12] by implementing both primary and secondary control in the LC. Each DG needs to collect measurements from other DGs and adopts the averaged values to achieve control. It is noticed that MGCC is still essential in the case of black start and other energy management processes.

Due to the dependence on the communication network, the reliability of MG operation could be disrupted once the vulnerabilities are exploited by attackers. For example, unsecured communication protocols lacking built-in encryption capabilities, such as Modbus and DNP3 [13], can be exploited by attackers. More specifically, denial-of-service (DoS) can overwhelm the target system by flooding it; Man-in-the-middle-based false data injection attacks (FDIAs) could intercept process communication to falsify the field devices which demonstrates in [14] within a laboratory environment. The system impacts of cyberattacks have been investigated on ac MG under different communication configurations. The authors in [15] examine the varying performance of a centralized communication-based MG under DoS attacks with different launch times and durations. Although the effect on system frequency, voltage, and active power is demonstrated, the attack model is based on a basic mechanism without considering more sophisticated attackers with advanced capabilities to implement FDIAs or other types of attacks. For a MG with distributed communication configuration, an impact assessment of FDIAs, replay attacks, and DoS attacks against transmitted frequency signal is performed in [16]. Curerent works focus on MGs during islanded mode while little research has been conducted during the grid-connected operation, as the dominant operated mdoe, let alone considering scenarios of FDIAs against communication channels.

It is crucial to identify such threats that could disrupt system operation in the early stage. Two approaches, model-based and data-driven methods have been applied for MG cyberattack detection in islanded operations. Regarding model-based approaches, residual-based [17] or the observer-based model [18], [19], [20] are utilized. However, the model-based detection algorithm may be challenging to design and implement in large-scale and complicated real-world applications [21]. Therefore, data-driven methods are leveraged as a promising option which is easy to scale up and not required the system model and parameters. For example, in dc MG with a distributed communication network, FDIAs on current and voltage sensor measurements can be uncovered after comparison with the estimated value based on artificial neural network (ANN) [22], [23] or nonlinear auto-regressive exogenous neural network [24]. Considering the limitation of the traditional statistical detectors such as χ^2, the article [25] presented a long-short-term-memory (LSTM) based detection method to identify the stealthy attack against sensor measurements and actuator signals in distributed dc MG. Regarding ac MG, as presented in [26], the FDIAs on the measurements can be captured by utilizing the proposed deep learning-based multi-label classification method during islanded operation with an overall accuracy of over 90%. Although the cyberattacks against measurements during islanded operations are adequately addressed by leveraging data-driven methods, the lack of a detection approach regarding islanded and grid-connected operations by considering the communication vulnerabilities is the remaining risk of MG operation.

In addition, the recognition of cyberattacks from faults is essential since incorrect classification may result in operational failure [27]. However, limited detection methods provide the feature to differentiate them [28]. Moreover, some faults are challenging to be detected, such as high-impedance faults (HIF) where fault currents are below the overcurrent thresholds [29]. The frequent occurrence and difficulty in detection could make the system exposed to cascading failures [30]. Although IEEE 1547-2018 [31] specifies tripping levels of frequency and voltage during DERs' interconnection and interoperability with an electrical grid which enhances the system reliability and reduces the risks of severely impairing physical equipment, most HIFs or deliberately designed FDIAs by sophisticated attackers could still bypass the overcurrent or IEEE 1547-2018 based protection functions and remain as potential threats to MG.

To address the challenges stated above, a data-driven cyberphysical anomaly detection for AC MGs with GFM inverters during islanded and grid-connected operations is proposed, which has not been researched yet. Specifically, comprehensive impact assessments are performed based on a developed system model with steady and dynamic transients in normal operation, HIFs at different locations, as well as FDIAs against different numbers of communication channels between MGCC and LCs. The proposed LSTM-based anomaly detection approach could effectively identify certain HIFs and FDIAs which could bypass the protection functions.

The rest of the article is organized as follows. Section II presents the system configuration of GFM inverter-based MG with dual operation modes and demonstrates its potential cyberphysical vulnerabilities. Regarding the observed vulnerabilities, comprehensive impact assessments of HIFs and FDIAs against MG in dual operation modes are evaluated in Section III based on real-time simulation results. The LSTM-based data-driven anomaly detection approach is proposed in Section IV. Finally, Section V concludes the article.

II. INTRODUCTION OF HIERARCHICAL CONTROL BASED MG WITH CYBERPHYSICAL VULNERABILITIES

A GFM-inverter based MG system with centralized communication network and hierarchical control is introduced in this section. Meanwhile, protection functions are applied to hierarchical control against abnormal conditions that violate IEEE 1547-2018 protection standard as well as inverter overcurrent threshold. Moreover, the vulnerabilities in cyberphysical layer that can bypass the protection functions are specified respectively.

A. SYSTEM CONFIGURATION AND MG CONTROL

The system configuration is demonstrated as shown in Fig. 1, which leverages a centralized communication where the LC located at each inverter communicates with the MGCC to obtain the control commands. In order to accomplish grid-connected and islanded operation, MG control presented in [10] is utilized here which consists of primary, secondary, and tertiary control. During islanded operation, primary and secondary control are mandatory while three levels are required to achieve grid-connected mode in the GFM-inverter based MG.

1) PRIMARY CONTROL

Droop control is employed in primary control to regulate the real power output via $P-\omega$ droops and reactive power output via $Q-V$ droops, respectively. ω and V are the angular frequency and magnitude of the inverter output voltage. As described by (1), k_P and k_Q are the droop coefficients, representing the linear relationship between P to ω and Q to V. By adjusting ω and V, the output power P and Q can be controlled accordingly. Moreover, $\Delta\omega$ and Δv are the compensation components provided by the secondary control.

$$\begin{aligned}\omega &= \omega^* - k_P \cdot (P - P^*) + \Delta\omega \\ V &= V^* - k_Q \cdot (Q - Q^*) + \Delta v\end{aligned} \tag{1}$$

2) SECONDARY CONTROL

The MG voltages at point of common coupling (PCC) $(\omega_{\text{pcc}}, V_{\text{pcc}})$ need to be regulated to predefined reference values $(\omega_{\text{pcc}}^*, V_{\text{pcc}}^*)$ to meet islanded or grid-connected operation requirement. Thus PI controllers are utilized to generate the compensation signal $\Delta\omega$ and Δv, as expressed in (2).

$$\begin{aligned}\Delta\omega &= k_{P\omega}\left(\omega_{\text{pcc}}^* - \omega_{\text{pcc}}\right) + k_{I\omega}\int\left(\omega_{\text{pcc}}^* - \omega_{\text{pcc}}\right)dt \\ \Delta v &= k_{Pv}\left(V_{\text{pcc}}^* - V_{\text{pcc}}\right) + k_{Iv}\int\left(V_{\text{pcc}}^* - V_{\text{pcc}}\right)dt\end{aligned} \tag{2}$$

3) TERTIARY CONTROL

Before connecting to the utility grid, the phase angle of grid θ_{g} and MG θ_{pcc} need synchronization to smoothen the MG transient behavior during the mode transfer from islanded to grid-connected operation. The generated control signal $\Delta\omega'$ is expressed in (3) and will be added to $\Delta\omega$ in the secondary control. Once MG switched to the grid-connected mode, the power flow between MG and the utility grid can be managed by tertiary control, which is expressed in (4). By updating the MG voltage reference (V_{pcc}^*, ω_{pcc}^*), the injected power from MG to grid P_{g} and Q_{g} is regulated to the reference value P_{g}^* and Q_{g}^*.

$$\Delta\omega' = k_{P\omega'}\left(\theta_{\text{g}} - \theta_{\text{pcc}}\right) + k_{I\omega'}\int\left(\theta_{\text{g}} - \theta_{\text{pcc}}\right)dt \tag{3}$$

$$\omega_{\text{pcc}}^* = k_{Pgp}\left(P_{\text{g}}^* - P_{\text{g}}\right) + k_{Igp}\int\left(P_{\text{g}}^* - P_{\text{g}}\right)dt$$

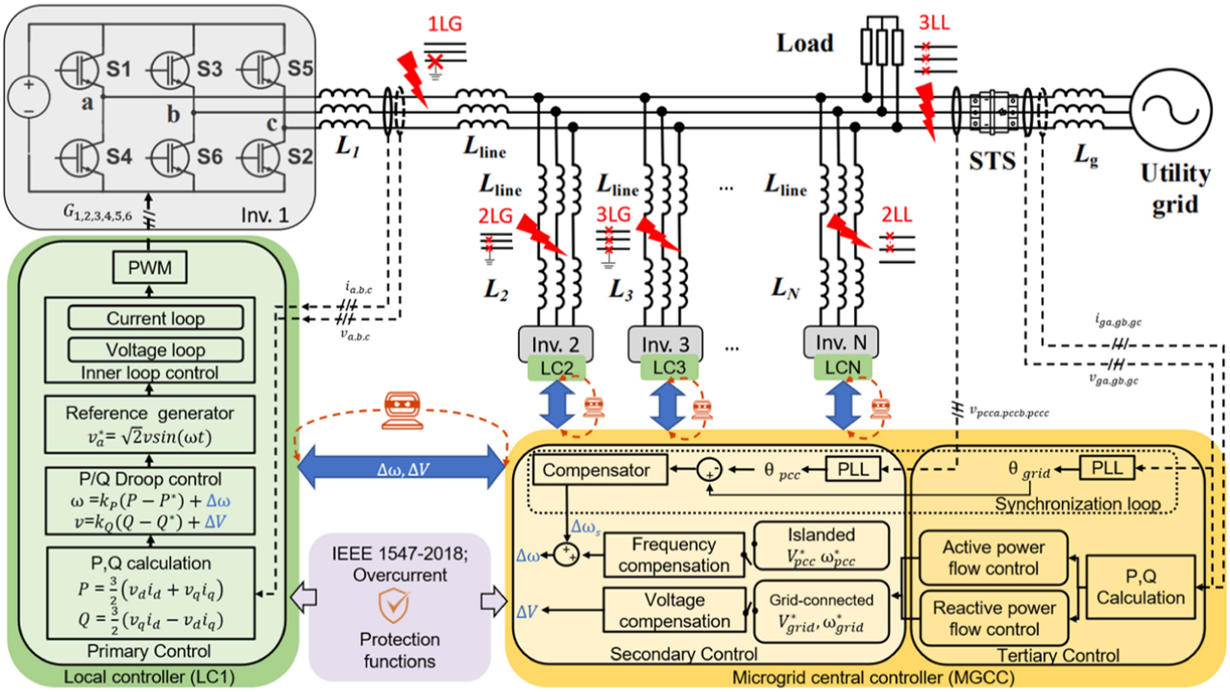


FIGURE 1. System configuration of GFM inverter-based MG with existing physical vulnerabilities (faults) and cyber vulnerabilities (cyberattacks).

$$V_{\text{pcc}}^{*} = k_{Pgq}\left(Q_{\text{g}}^{*} - Q_{\text{g}}\right) + k_{Igq}\int \left(Q_{\text{g}}^{*} - Q_{\text{g}}\right) dt \qquad (4)$$

B. ABNORMAL CONDITIONS IDENTIFIED BY PROTECTION FUNCTIONS

In Fig. 1, the protection functions have been applied to a hierarchical control based MG against abnormal conditions that can be identified by IEEE 1547-2018 protection standard and inverter overcurrent threshold. IEEE 1547-2018 indicates the minimum equipment capability required in response to abnormal situations such as over/under voltage and over/under frequency fault scenarios. Particularly, there are Category I, II, and III depending on the system's characteristics and capabilities. Category I is adopted in this article since it defines the essential bulk power system stability/reliability requirement by all DER technologies that are commonly used today [32]. The corresponding protection trip values and fault clearing timing of category I are listed in Table 1, where there are two overvoltage trip functions, OV1 and OV2, and two undervoltage trip functions, UV1 and UV2. Similarly, two overfrequency trip functions, OF1 and OF2, and two underfrequency trip functions, UF1 and UF2. In addition, overcurrent protection for the inverter-based DERs to avoid permanent damage to power semiconductors during faults is followed with a 2 p.u threshold [33], [34].

Hence, abnormal system operation and inverter from overcurrent conditions will be identified once triggering the system level protection based on IEEE 1547-2018 and local overcurrent thresholds, respectively. Moreover, other remaining cyberphysical threats that can bypass the protection functions are also considered and specified as follows.

TABLE 1. DER Response to Abnormal Voltage and Frequency Based on IEEE 1547-2018 Category I

Shall trip function	Voltage (p.u. of nominal voltage)	Clearing time (s)
OV2	1.20	0.16
OV1	1.10	2.0
UV1	0.70	2.0
UV2	0.45	0.16
	Frequency (Hz)	Clearing time(s)
OF2	62.0	0.16
OF1	61.2	300.0
UF1	58.5	300.0
UF2	56.5	0.16

C. CYBERPHYSICAL VULNERABILITIES BYPASS PROTECTION FUNCTIONS

There exist cyberphysical vulnerabilities in the MG, such as physical faults and cyberattacks, that remain undetected by bypassing protection functions. In respect of physical faults, the created fault path may lead to overcurrent, over/undervoltage, or reversed power flow which could interrupt normal operation, cause a power outage, or even damage equipment. Two main categories of faults are *i)* open circuit fault and *ii)* short circuit fault. Open circuit fault refers to conductor breaking which creates an ultra-high fault impedance to interrupt the current flow. A short circuit is a fault introduced by the insulation failure which may involve one or more phases to earth or occur between phases. This article will focus on the short circuit fault since it could be more destructive.

In the GFM inverter-based MG, overcurrent protection could effectively detect low-impedance faults with high overcurrent. However, HIF brings risks to maintaining normal operation and protecting the system. In our case, the overcurrent protection is 2 p.u. and thus impedance over 50% will be considered as HIFs. Regarding fault locations, HIFs may occur on the inverter side or the PCC side, as demonstrated in Fig. 1. The fault types include single-phase line-to-ground fault (1LG), two-phase line-to ground-fault (2LG), three-phase line-to-ground fault (3LG), two-phase line-to-line fault (2LL), and three-phase line-to-line fault (3LL).

Based on the microgrid control structure, the master-slave communication architecture between the central control and local controls is commonly applied, where the protocols including DNP3, IEC 61850, and Modbus are utilized [35]. Regarding the vulnerabilities in the cyber layer, the unsecured communication network (e.g., communication protocols lacking built-in encryption capabilities, insufficient firewalls, and intrusion detection) can be exploited by the attackers. The literature demonstrates how the DNP3 [36], IEC 61850 [37], and Modbus [38] protocols can be compromised respectively. When the communicating agents, each LC and MGCC, are intercepted, the transferred data ΔX, including $\Delta\omega$ and ΔV, can be manipulated through FDIAs and then bypass the protection functions. As a result, the primary droop control scheme will be deceived with altered value and then generate misguided reference value (v_a^*) for the inner loop control.

Four attack signals including random, scaling, sine, and continuous pulse signals are modeled in (5-8), where ΔX is the real value, $\Delta X a$ is the altered value and the attack duration is represented by T_a.

1) RANDOM ATTACK SIGNAL

The random attack signal follows the Gaussian distribution with mean μ and variance σ^2. The transmitted data under attack is expressed in (5).

$$\Delta X_a = \begin{cases} rand(t) + \Delta X & \text{t} \in T_a \\ \Delta X & \text{otherwise} \end{cases} \tag{5}$$

2) SCALING ATTACK SIGNAL

This type of attack could temporarily change the signal by using a scaling attack factor γ_{sca}, as shown in (6).

$$\Delta X_a = \begin{cases} \gamma_{sca} * \Delta X & \text{t} \in T_a \\ \Delta X & \text{otherwise} \end{cases} \tag{6}$$

3) SINE ATTACK SIGNAL

A sinusoidal signal with amplitude γ_{sin} and frequency ω_{sin} is utilized to alter the original data ΔX in (7).

$$\Delta X_a = \begin{cases} \gamma_{sin} * \sin(\omega_{\text{sin}} t) * \Delta X & \text{t} \in T_a \\ \Delta X & \text{otherwise} \end{cases} \tag{7}$$

TABLE 2. MG Simulation Model Parameters

Parameters	Value
$S_{base3\phi}$	60 kVA
V_{baseLL}	480 V
I_{baseLL}	72.2 A
Z_{baseLL}	3.8 Ω
Local load range, P_L	4 $\sim$ 40 kW
Power penetration to grid range, P_P	2 $\sim$ 20 kW
Grid inductance,L_g	$0.2mH$(2.0% p.u.)
Inverter filter inductance,$L_{1,2,3,4}$	$0.3mH$(3.0% p.u.)
Line inductance,L_{line}	$0.01mH$(0.1% p.u.)

4) CONTINUOUS PULSE ATTACK

The attacker could also inject the malicious vectors repeatedly. The transmitted data is transferred into a periodic square wave signal, as described in (8), where γ_c is the change ratio, T_a is the period and D is the duty cycle.

$$\Delta X_a = \begin{cases} \Delta X & \text{t} \in [nT_a, (n+D)T_a] \\ \gamma_c * \Delta X & \text{t} \notin [(n+D)T_a, (n+1)T_a] \end{cases} \tag{8}$$

III. IMPACT ASSESSMENT OF CYBERPHYSICAL VULNERABILITIES

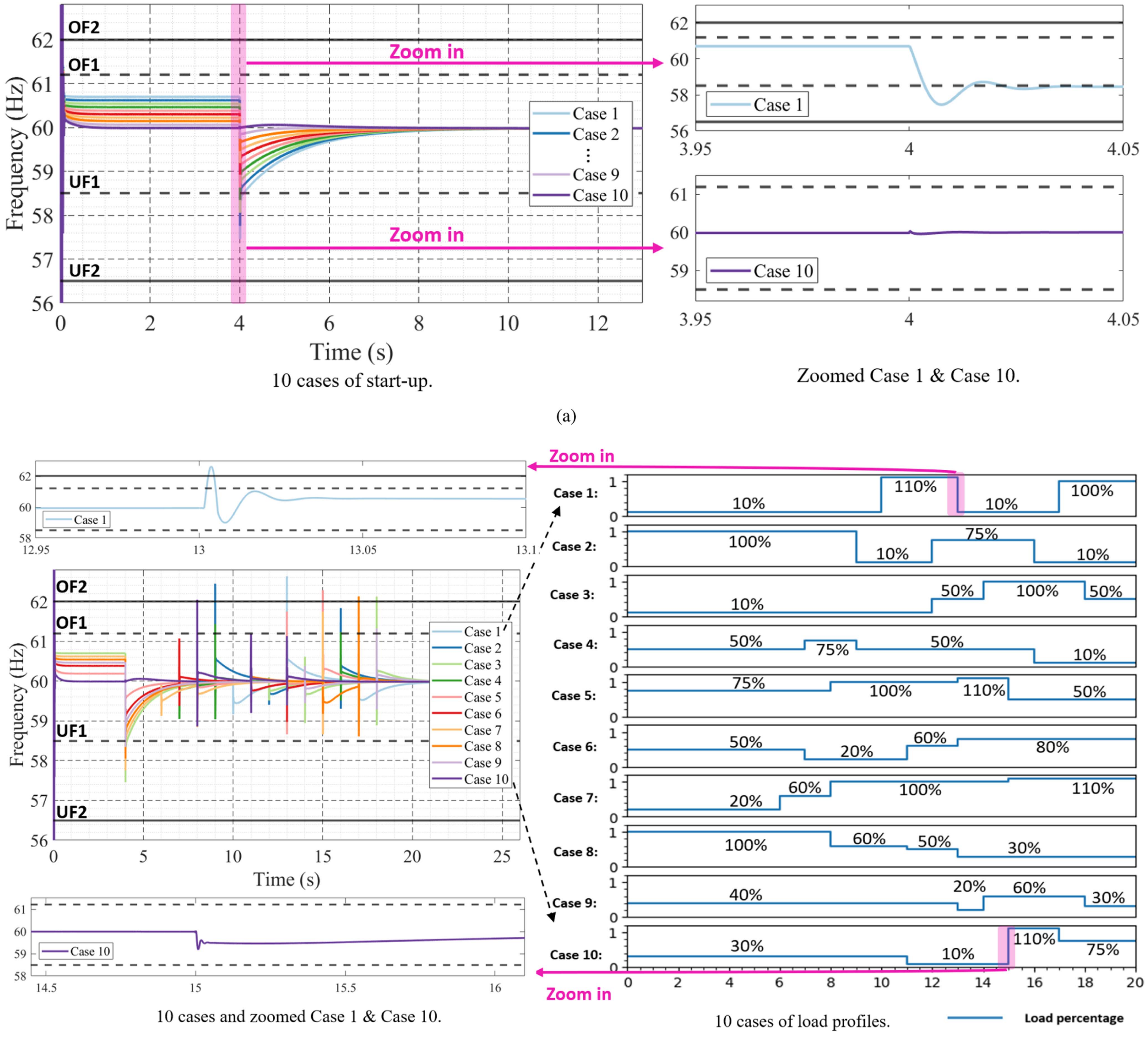
The simulation model of the MG system depicts in Fig. 1 is developed, where N is selected to 4 and there are 4 communication channels in total between MGCC and LCs. The key simulation specifications are listed in Table 2. Comprehensive impact assessments are provided in this section addressing two operation modes (islanded and grid-connected) with three operating conditions (normal, HIFs, and FDIAs). All study cases are conducted in a real-time environment via OPAL-RT.

A. SYSTEM ASSESSMENTS OF NORMAL OPERATION

In order to obtain the data of the system in normal operation, steady state and dynamic transient cases are considered in islanded and grid-connected modes. Islanded cases include i) start-up in different load conditions, and ii) dynamic change of loads. Grid-connected cases include i) different load conditions and ii) power penetration levels during the connection, as well as iii) a dynamic change of loads or power penetration.

1) NORMAL OPERATION DURING ISLANDED MODE

10 Cases of MG start-up with different loads from 10% (4 kW) to 100% (40 kW) of the rated load, are examined. As shown in Fig. 2(a), the fundamental frequency can vary between 57.5 Hz and 60.75 Hz at t =0s when the primary control is activated. The light load condition in Case 1 raises the frequency above 60 Hz during steady state, while the frequency is slightly lower than 60 Hz with 100% rated load in Case 10. The frequency of all cases listed can then be compensated to 60 Hz by applying the secondary control at 4s. The frequency transients of Case 1 and 10 at 4 s are zoomed on the right side. According to the over/under frequency protection specified in Table 1, the solid black line refers to UF2/OF2 and the dotted black line denotes UF1/OF1. Among all cases, OF1, OF2, and UF2 are not reached, and UF1 will not be triggered either since the duration is shorter than 300 s.



10 cases of start-up.

Zoomed Case 1 & Case 10.

(a)

10 cases and zoomed Case 1 & Case 10.

10 cases of load profiles.

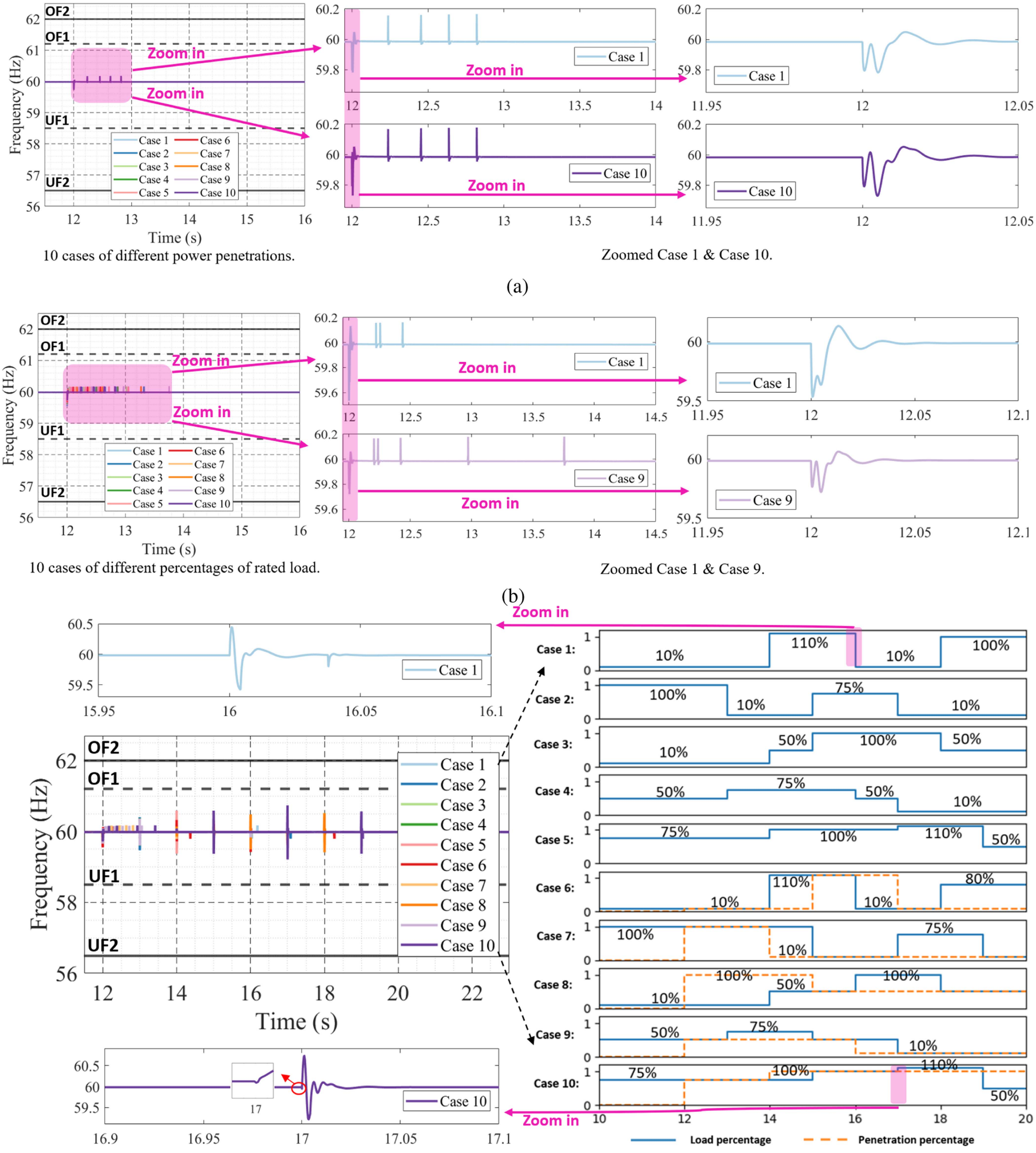
(b)

FIGURE 2. Fundamental frequency response of normal operation during islanded mode. (a) 10 cases of start-up corresponding to 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, 100% of rated load and (b) 10 cases of dynamic change of loads with different load profiles.

The dynamic behavior of islanded mode during load change transients is examined using 10 cases of different load profiles depicted on the right of Fig. 2(b). The cases feature different timing and degree of load change. Several typical loads are selected, where 10%, 20%, 30% representing light loads, 50% as medium load, 60%, 75%, 80% as heavy load, 100% referring to full load, and 110% indicating overload. Taking Case 1 as an example, the loads change from 10% to 110% at t=10s. Then the loads drop back to 10% at t = 13s. Finally, the loads ramp up to full load 100% at t = 17s and keep unchanged. It should be noted that all load change events occur after t = 4s when the secondary control is enabled. The frequency variation corresponding to all 10 cases is shown on the left plot of Fig. 2(b). More specifically, the peak frequency, 62.63Hz, is caused by the load reduction from 110% to 10% in Case 1, while a direct drop of the frequency to 59.2Hz is obtained in Case 10 with the increase of load consumption from 10% to 110% as shown in the upper and lower zoomed figure. Although the varying frequency is beyond the threshold of UF1, OF1, or OF2 in several cases, the clearing time is insufficient to trigger the frequency protection function.

2) NORMAL OPERATION DURING GRID-CONNECTED MODE

The impacts of different loads during grid-connected operation are evaluated with 10 cases from 10% (4 kW) to 100% (40 kW) of the rated load, MG is connected to the grid at



10 cases of different power penetrations.

Zoomed Case 1 & Case 10.

(a)

10 cases of different percentages of rated load.

Zoomed Case 1 & Case 9.

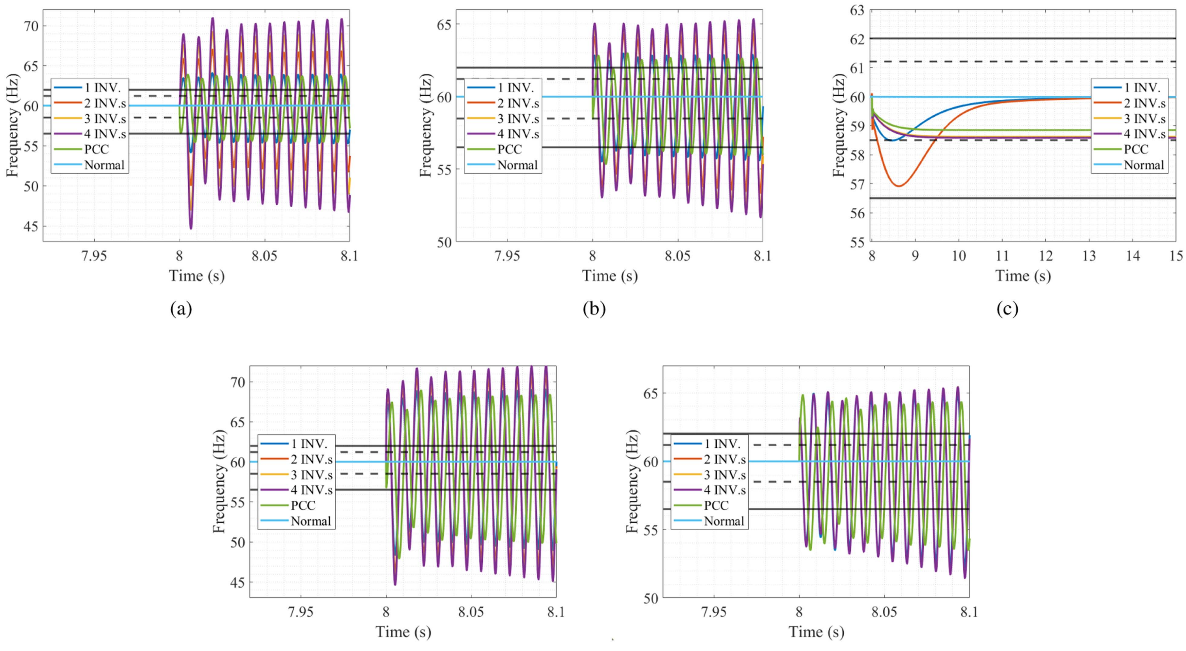
(b)

10 cases and zoomed Case 1 & Case 10.

10 cases of load profiles.

FIGURE 3. Fundamental frequency response of normal operation during grid-connected mode. (a) 10 cases corresponding to 10%, 20%, 30%, 40%, 50%, 60%,70%, 80%, 90%,100% of rated load, (b) 10 cases corresponding to 10%, 20%, 30%, 40%, 50%, 60%,70%, 80%, 90%,100% of penetration power, and (c) 10 cases of dynamic change of loads with different load profiles.

t=12s, where Case 10 under full load fluctuates most drastically in frequency but there is no violation of the frequency thresholds, as is shown in Fig. 3(a). Moreover, different power penetration from MG to the utility grid implemented by adjusting power setpoints in MGCC should be addressed in grid-connected mode. The influence on the frequency of 10 different power penetration levels from 10% (2 kW) to 100% (20 kW) of the rated power is investigated. As shown in Fig. 3(b), different cases result in different frequency responses without surpassing any frequency limit. In addition, changes of local loads or power penetration to the utility grid are considered in 10 cases demonstrated on the right plot of Fig.



(a)

(b)

(c)

(d)

(e)

FIGURE 4. Fundamental frequency during islanded operation regarding five HIFs: (a) phase A LG, (b) phase AB LG, (c) 3 phase LG, (d) phase AB LL, and (e) 3 Phase LL.

TABLE 3. Critical Values of HIFs in Islanded Mode

Type of faults Locations	1LG $(p.u.)$	2LG $(p.u.)$	3LG $(p.u.)$	1LL $(p.u.)$	3LL $(p.u.)$
Inv.1	**52.08%**	**52.08%**	**52.08%**	**52.08%**	**52.08%**
Inv.1,2	**52.08%**	**52.08%**	**52.08%**	**52.08%**	**52.08%**
Inv.1,2,3	**52.08%**	**52.08%**	**260.42%**	**104.17%**	**78.13%**
Inv.1,2,3,4	**52.08%**	**52.08%**	**338.54%**	**130.21%**	**104.71%**
PCC	**52.08%**	**52.08%**	**104.17%**	**52.08%**	**52.08%**

TABLE 4. Critical Values of HIFs in Grid-Connected Mode

Type of faults Locations	1LG $(p.u.)$	2LG $(p.u.)$	3LG $(p.u.)$	1LL $(p.u.)$	3LL $(p.u.)$
Inv.1	**52.08%**	**52.08%**	**52.08%**	**78.13%**	**104.17%**
Inv.1,2	**52.08%**	**78.13%**	**78.13%**	**156.25%**	**208.33%**
Inv.1,2,3	**78.13%**	**104.17%**	**104.17%**	**234.38%**	**286.46%**
Inv.1,2,3,4	**104.17%**	**130.21%**	**156.25**	**234.38%**	**364.58%**
PCC	**52.08%**	**52.08%**	**52.08%**	**104.17%**	**104.17%**

3(c), solely load changes (solid blue line) considered in Cases 1 to 5 and power penetration changes (dotted orange line) included in Cases 6 to 10. The frequency response of all cases is shown on the left plot, where all the transients are within thresholds. Regarding Case 1, a fluctuation is observed between 60.5 Hz to 59.4 Hz when a load change from 110% to 10% is initialized at t = 16 s. Both peak frequency, 60.74 Hz, and lowest frequency, 59.21 Hz, are obtained when loads change from 100% to 110% in Case 10 at t = 17 s.

B. IMPACT ASSESSMENTS OF HIFS

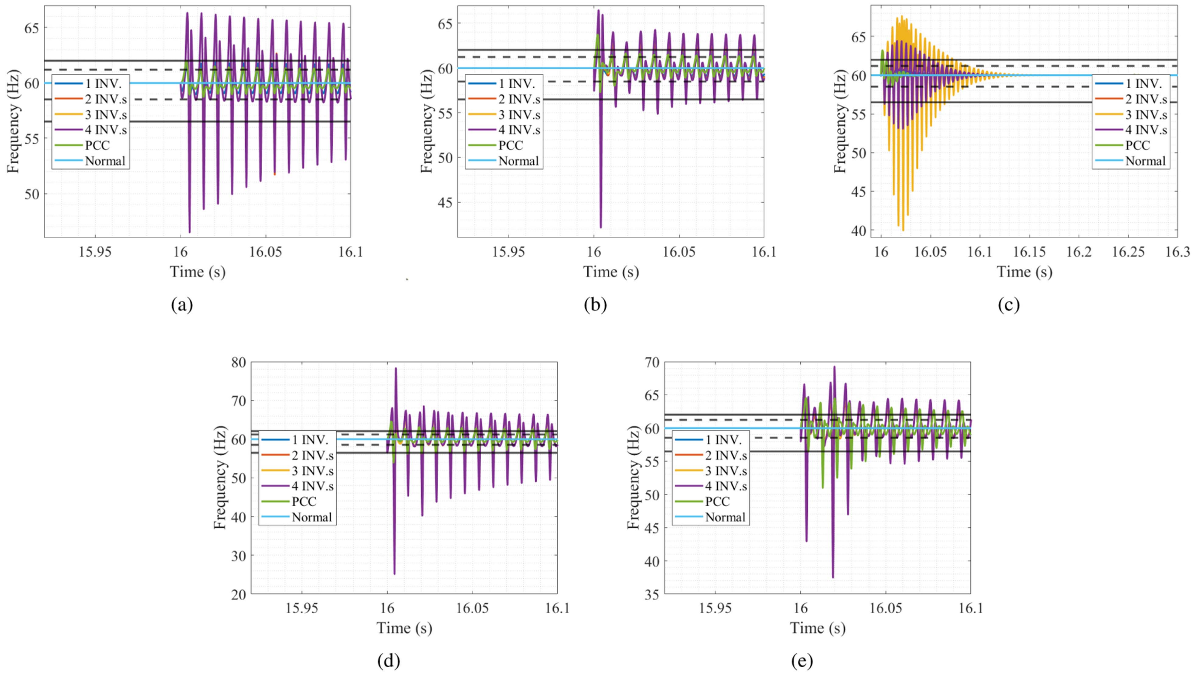
Fig. 1 demonstrates 5 short circuit HIFs which are 1LG, 2LG, 3LG, 2LL, and 3LL. Meanwhile, HIFs could occur on any inverter output or at the PCC point. When each inverter is considered equivalent, 5 fault locations can represent all possible locations. Thus, 25 HIF scenarios are studied herein by combining fault types and fault locations. After running real-time simulations, the critical fault impedance that not triggering protection is determined, as shown in Table 3 for islanded mode and Table 4 for grid-connected mode.

1) HIFS IMPACTS DURING ISLANDED MODE

The impacts of HIFs on the fundamental frequency at PCC are illustrated in Fig. 4. Significant frequency distortion can be identified in all cases after fault inception at t=8 s. In general, the impact is heavier when more inverters are involved in faults. Fig. 4(c) shows the worst case with the frequency fluctuating between 44.61 Hz to 71.69 Hz in the case of 2LL fault occurring on all inverters. While the symmetrical 3LG fault has the slightest impact, where the frequency will recover to normal after a temporary drop, except the case involving 4 inverters cannot recover back with the frequency kept at 57.65 Hz.

2) HIFS IMPACTS DURING GRID-CONNECTED MODE

Fig. 5 demonstrates the grid-connected fault scenarios, where faults are triggered at t = 16 s. Similar to islanded cases, the frequency fluctuation is larger with more inverters being engaged. The worst case is the 1LL fault on 4 inverters, where the frequency ranges from 25.10 Hz to 78.35 Hz.



(a)

(b)

(c)

(d)

(e)

FIGURE 5. Fundamental frequency during grid-connected operation regarding five HIFs: (a) phase A LG, (b) phase AB LG, (c) 3 phase LG, (d) phase AB LL, and (e) 3 Phase LL.

TABLE 5. Values of Attack Signals in Islanded Mode

Type of attacks / Num. of Comm.	Random	Scaling	Sine	Pulse
	μ, σ^2	γ_{sca}	γ_{sin}, ω	γ_c, T, DT
1,2,3,4	3,10	3	1,5	300,300,20
	5,10	200	6,4	200,300,10

TABLE 6. Values of Attack Signals in Grid-Connected Mode

Type of attacks / Num. of Comm.	Random	Scaling	Sine	Pulse
	μ, σ^2	γ_{sca}	γ_{sin}, ω	γ_c, T, DT
1,2,3,4	3,10	1.3	1,5	2,20,4
	5,6	1.5	1,8	2,20,10

C. IMPACT ASSESSMENTS OF FDIAS

The cyberattack impact on MG is examined in terms of 4 FDIAs based attack signals: random; scaling; sine; and continuous pulse. Each attack signal utilizes 2 sets of parameters to generalize the analysis. The communication channel between MGCC and any LC within the inverter can be compromised individually. When each inverter is considered equivalent, 4 cases with a different number of compromised communication channels can represent all cases. The attacks scenarios are summarized by cooperating the number of compromised communication channels and different attack signals, which is specified in Table 5 for islanded and Table 6 for grid-connected, respectively.

1) FDIAS IMPACTS DURING ISLANDED MODE

The disturbance on PCC frequency caused by FDIAs cases is demonstrated in Fig. 6, when an attack is activated at t=8 s. With more communication channels being compromised, the impact on frequency will be heavier. The random signal against 4 communication channels could increase the frequency to 60.5Hz instantaneously. While the scaling signal attack causes a slight and temporary increase in the frequency before returning to normal. In the case of the sine signal attack, the frequency oscillation may diverge and ultimately destabilize the system if no corrective measures are taken. A periodic fluctuation in the frequency exists after being attacked by a continuous pulse signal.

2) FDIAS IMPACTS DURING GRID-CONNECTED MODE

Compared with islanded cases, the MG in grid-connected mode becomes more resilient against FDIAs since the connected grid improves the MG stability. As shown in Fig. 7(a), the frequency fluctuation is limited between 59.96 Hz to 60.02 Hz under random signal based FDIAs. Even fewer frequency disturbance is caused temporarily by initialing the scaling signal attack, as can be seen in Fig. 7(b). As the most severe case among 4 attack signals presented in Fig. 7(c), the frequency is over 68.86 Hz around 16.8 s when 4 communication channels compromised by FDIAs and the frequency reaches 63 Hz with 3 communication channels under attack at t = 16.97 s. The impact on frequency from the continuous pulse signal attack is shown in Fig. 7(d), where a periodic variation of the frequency is induced between 59.977 Hz to 59.998 Hz.

IV. LSTM BASED DATA-DRIVEN ANOMALY DETECTION

The frequency, voltage, and current at PCC point represent the system-level operation conditions of MG. However, the

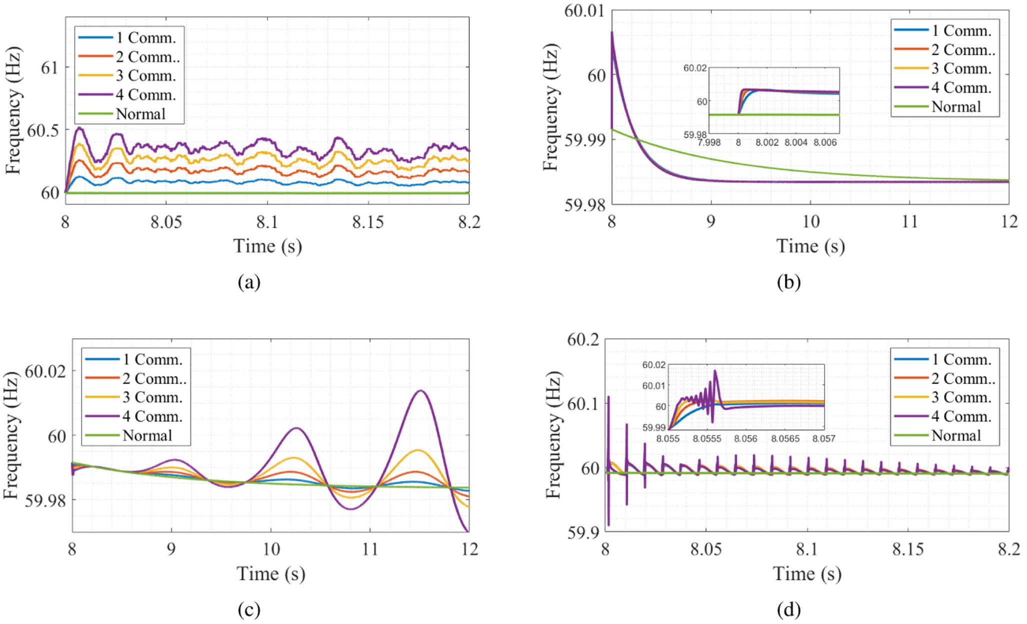


FIGURE 6. Fundamental frequency during islanded operation regarding four cyberattack signals (a) random, (b) scaling, (c) sine, and (d) continuous pulse.

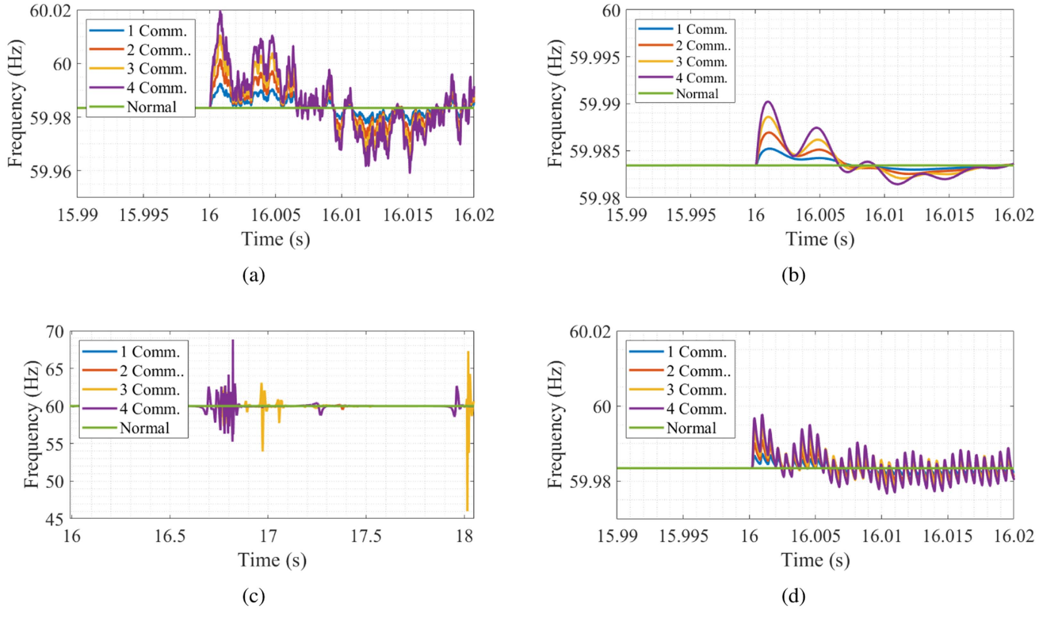


FIGURE 7. Fundamental frequency during grid-connected operation regarding four cyberattack signals (a) random, (b) scaling, (c) sine, and (d) continuous pulse.

zero PCC current during islanded makes it difficult to detect anomalies in a unified algorithm for both islanded and grid-connected operations. Furthermore, as demonstrated in Fig. 8, phase A voltage is slightly increased for around 0.06 p.u. under the random signal against 4 communication channels at 8.0165s, 3 and 1 tiny spikes on phase C and A voltage are observed respectively under the continuous pulse signal attack, and the voltage variation regarding scaling signal and sine signal attack are ignorable. Therefore, the PCC frequency is utilized to extract the operation features of MG to identify the HIFs and FDIAs.

In order to obtain sufficient data to perform the training process, the data corresponding to different operation conditions detailed Section III are collected. There are 150 data sets in total, which include 50 normal cases, 50 faults cases, and 50 attack cases. Among 50 cases, 25 are for islanded

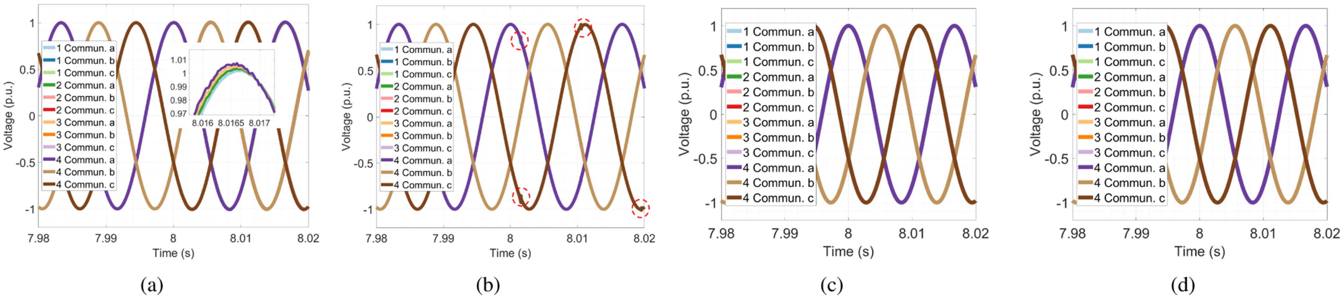


FIGURE 8. Voltage during islanded operation regarding four cyberattack signals: (a) random, (b) continuous pulse, (c) scaling, and (d) sine.

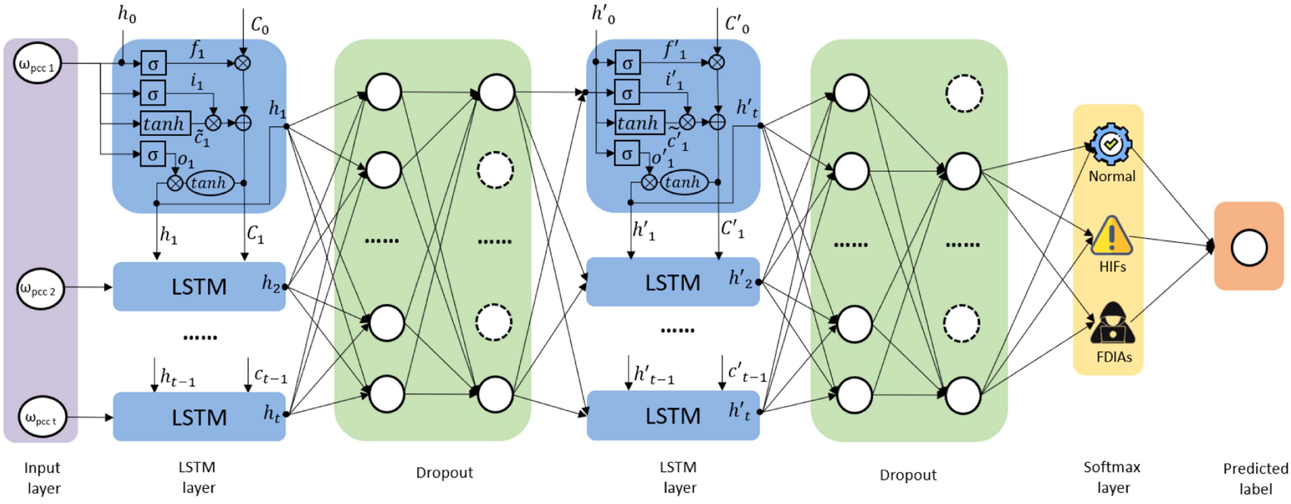


FIGURE 9. The structure of LSTM-based multi-class anomaly classification.

and 25 are for grid-connected operation. The case number for the three scenarios are similar to ensure sufficient data for each scenario. Each data set contains 666,667 data points and depicts MG operation of 20s with the time step of $3e-5$s. The data sets are split into 80% (120) for training, 10% (15) for validation, and 10% (15) for testing.

A. LSTM NETWORK

In order to achieve the detection and classification of the multi-class containing normal, HIFs, and FDIAs, LSTM is deployed considering its advantages of classifying, processing, and making predictions based on time series data [39]. The time series PCC frequency fed into the input layer of data-driven anomaly detection scheme shown in Fig. 9. Furthermore, the tschemes includes 2 LSTM layers, 2 dropout layers to avoid model overfitting by ignoring selected neurons, a softmax layer to determine the probability distribution over each predicted label, and a predicted output. Specifically, LSTM leverages gating mechanism which includes the forget gate f_t, input gate i_t, and output gate o_t, as formulated in (9), where σ the sigmoid activation function, h_{t-1} the previous hidden state from the $t-1$ cell, ω_{pcct} the current time series input. The hidden state at t is generated as $h_t = o_t \cdot \tanh(c_t)$, where new cell state is derived by $c_t = f_t \cdot c_{t-1} + i_t \cdot \tanh(w_c[h_{t-1}, x_t] + b_c)$. The tanh refers to hyperbolic tangent activation function and c_{t-1} is the previous cell state. w_f, w_i, w_o, w_c the weight matrices, and b_f, b_i, b_o, b_c bias vectors.

$$\begin{aligned} f_t &= \sigma\left(w_f\left[h_{t-1}, \omega_{pcct}\right] + b_f\right) \\ i_t &= \sigma\left(w_i\left[h_{t-1}, \omega_{pcct}\right] + b_i\right) \\ o_t &= \sigma\left(w_o\left[h_{t-1}, \omega_{pcct}\right] + b_o\right) \end{aligned} \tag{9}$$

To address the multi-class classification problem, categorical cross-entropy is utilized as the loss function shown in (10), y_i and $\hat{y}_i$ are the ground truths and the predicted class for a sample i, respectively.

$$L = -\sum_{i=1}^{N} y_i \cdot \log \hat{y}_i \tag{10}$$

B. HYPERPARAMETER OPTIMIZATION

To optimize the overall accuracy, different data sampling rates, hidden neurons number in LSTM layers, and batch size are evaluated. The data size increases with a higher data sampling rate. Scenario 1 (S1) has 13320 data points

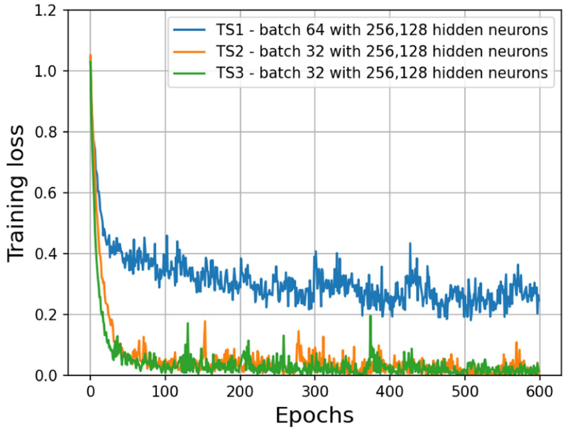


FIGURE 10. Optimal training loss for 3 scenarios with different configurations.

TABLE 7. Hyperparameters

Num. of hidden layers	2
Num. of hidden neurons	256, 128
Batch size	32
Learning rate (α)	1e-5
Optimizer	Adam
Max. epochs	600
Dropout	0.5

corresponding to 666 per second sampling. Scenario 2 (S2) and 3 (S3) have a lower sampling rate of 128 and 33 points per second, respectively. For each scenario, 3 hidden neuron numbers (256/128, 128/64, and 64/32) and 3 batch sizes (32, 64, and 128) are utilized to verify the training and validating performance. The configuration with optimal performance during the validation process will be selected. S1 has the lowest losses when hidden neurons number are 256/128 and the batch size is 64. While the optimized configuration of S2 is 256/128 hidden neurons and batch size of 32, and that of S3 is 256/128 hidden neurons and batch size of 32, as shown in Fig. 10. The training losses decrease with more epochs in all scenarios, which indicates an improving performance of the detection scheme. With the loss for S3 approaching zero, the predicted result is almost the true class. The corresponding hyperparameters are listed in Table 7.

C. PERFORMANCE METRICS AND COMPUTATIONAL EFFICIENCY

The performance of LSTM-based multi-class classification is evaluated based on the confusion matrix shown in Fig. 11(a). In the testing data set, there are 4 (0.27) normal cases, 7 (0.47) HIF cases, and 4 (0.27) FDIA cases. It can be seen that the predicted label matches the true label in all testing cases. Considering the limited data set size, the data-driven classification scheme may be sensitive to data splitting. In order to avoid the impact on the results caused by the data splitting, we choose 50 combinations with different splitting for training, validating, and testing. The pseudo-random is utilized and generated by the random state function, which implies the selection of a random combination. Thus 49 more schemes are derived based on different data-splitting configurations. It is found that the testing accuracy will vary between 80% to 100% and 3 confusion matrix examples are demonstrated in Fig. 11(b)–(d). Taking the worst scenario with 80% accuracy in Fig. 11(d) as an example, besides 12 correct predictions, there are 1 (0.067) wrong prediction which mistakes the normal case as FDIA, and 2 (0.13) wrong prediction which mistakes HIFs as FDIAs. Among all testing results, the accuracy is 100% in 21 cases (42%), 93.33% in 22 cases (44%), 86.67% in 5 cases (10%), and 80% in 2 cases (4%). The average accuracy of the LSTM-based multi-class classification scheme is 94.72%.

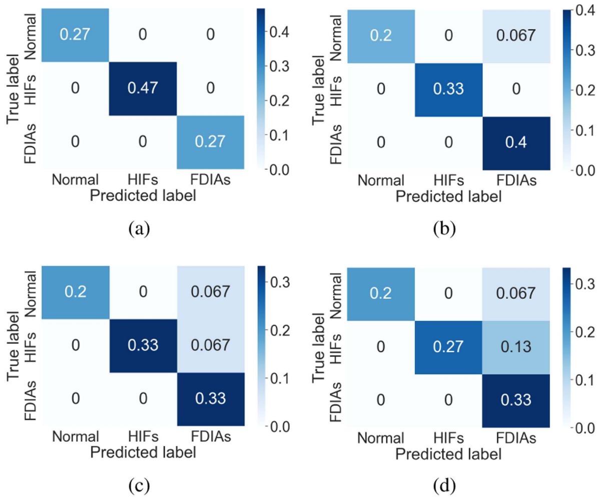


FIGURE 11. Confusion matrix for testing case with (a) 100% accuracy, (b) 93.33% accuracy, (c) 86.67% accuracy, and (d) 80.00% accuracy.

TABLE 8. Computational Efficiency of SC3

Neurons num. / Batch size	256,128		
	Train& validate (s)	Test (s)	Total (s)
32	**36.914**	**0.407**	**37.321**

The training, validating, and testing for each test case are performed on a x64-based processor with an Intel Core i7-10700K 3.8 GHz CPU and 32 GB memory. The computational efficiency is summarized in Table 8. Although the small batch size and large dimensions of hidden layers/neurons may slow down the overall efficiency, it only takes around 37.3s in total when the sampling rate is 33Hz. In addition, the low sampling rate of the proposed approach could bring benefits to the physical applications, where the noise in field data can be filtered out by adding an analog or digital filter. Furthermore, the communication bandwidth of the secondary control is quite low (down to 3 Hz[10]). Assume the int data type ($32bit$) is used to represent the two transmitted parameters (Δw, Δv), the required baud rate is $2 * 32bit * 3\text{Hz} = 192bps$. The commonly used communication protocols such as DNP3, Modbus, and IEC 61850 could reach higher speeds starting from *Kbps*. Meanwhile, the targets in the proposed detection method are stealthy fault/attacks, which have an unnoticeable and long-lasting influence on the system. Thus the detection method does not require a fast response. Thus communication delay impact on the proposed approach may be eligible.

V. CONCLUSION AND FUTURE WORK

In this article, the research gap is identified in the cyberphysical security of MG by detecting and differentiating cyber and physical vulnerabilities during both islanded and grid-connected modes. To bridge this gap, as the first study to address cyberphysical anomaly detection and classification during dual operation modes, this article i) exploited FDIAs against centralized communication networks between MGCC and LCs in a GFM inverter-based MG during two operation modes, ii) provided one of the most comprehensive impact assessments on normal operation, HIFs, and FDIAs based on real-time simulation results. iii) proposed an innovative data-driven anomaly detection approach to identify and classify HIFs and FDIAs which cannot trigger conventional protection functions, specifically overcurrent and IEEE 1547-2018 based protection functions. The proposed detection mechanism is verified with an average accuracy of 94.72%.

Considering a comprehensive dataset encompassing the key feature of normal, fault, and typical attacks covered in this article, a new type of attack should also be detected if the system response is significantly different from normal operations and faults. In future work, more attack scenarios will be considered to enhance the detection capability of the proposed approach. Furthermore, given the significant role of the GFL converters in grid-connected penetration, a mixed system with GFM and GFL inverters during grid-connected operation considering different control strategies, stability, fault/attack response as well as protection threshold will be explored with the proposed method in the future.

REFERENCES

[1] Y. Lin et al., “Research roadmap on grid-forming inverters,” National Renewable Energy Lab., Golden, CO, USA, Tech. Rep. NREL/TP-5D00-73476, 2020.

[2] J. Rocabert, A. Luna, F. Blaabjerg, and P. Rodriguez, “Control of power converters in AC microgrids,” *IEEE Trans. Power Electron.*, vol. 27, no. 11, pp. 4734–4749, Nov. 2012.

[3] R. H. Lasseter, Z. Chen, and D. Pattabiraman, “Grid-forming inverters: A critical asset for the power grid,” *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 8, no. 2, pp. 925–935, Jun. 2020.

[4] D. Pan, X. Wang, F. Liu, and R. Shi, “Transient stability of voltage-source converters with grid-forming control: A design-oriented study,” *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 8, no. 2, pp. 1019–1033, Jun. 2020.

[5] J. Matevosyan et al., “Grid-forming inverters: Are they the key for high renewable penetration?,” *IEEE Power Energy Mag.*, vol. 17, no. 6, pp. 89–98, Nov./Dec. 2019.

[6] “Harnessing smart power electronics to increase renewable energy penetration in tomorrow’s utility grid,” 2018. [Online]. Available: https://energy.sandia.gov/wp-content/uploads/2018/08/5_Jahns_2018_PE_Workshop.pdf

[7] J. Guerrero, L. de Vicuna, J. Matas, M. Castilla, and J. Miret, “A wireless controller to enhance dynamic performance of parallel inverters in distributed generation systems,” *IEEE Trans. Power Electron.*, vol. 19, no. 5, pp. 1205–1213, Sep. 2004.

[8] T. Kawabata and S. Higashino, “Parallel operation of voltage source inverters,” *IEEE Trans. Ind. Appl.*, vol. 24, no. 2, pp. 281–287, Mar./Apr. 1988.

[9] M. Chandorkar, D. Divan, and R. Adapa, “Control of parallel connected inverters in standalone AC supply systems,” *IEEE Trans. Ind. Appl.*, vol. 29, no. 1, pp. 136–143, Jan./Feb. 1993.

[10] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castilla, “Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization,” *IEEE Trans. Ind. Electron.*, vol. 58, no. 1, pp. 158–172, Jan. 2011.

[11] S. D’silva, M. Shadmand, S. Bayhan, and H. Abu-Rub, “Towards grid of microgrids: Seamless transition between grid-connected and islanded modes of operation,” *IEEE Open J. Ind. Electron. Soc.*, vol. 1, pp. 66–81, 2020.

[12] Q. Shafiee, J. M. Guerrero, and J. C. Vasquez, “Distributed secondary control for islanded microgrids—A novel approach,” *IEEE Trans. Power Electron.*, vol. 29, no. 2, pp. 1018–1031, Feb. 2014.

[13] T. H. Morris, S. Pan, and U. Adhikari, “Cyber security recommendations for wide area monitoring, protection, and control systems,” in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2012, pp. 1–6.

[14] Ö. Sen et al., “Investigating man-in-the-middle-based false data injection in a smart grid laboratory environment,” in *Proc. IEEE PES Innov. Smart Grid Technol. Europe*, 2021, pp. 01–06.

[15] S. Liu, Z. Hu, X. Wang, and L. Wu, “Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks,” *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4066–4075, Jul. 2019.

[16] S. Rath, D. Pal, P. S. Sharma, and B. K. Panigrahi, “A cyber-secure distributed control architecture for autonomous AC microgrid,” *IEEE Syst. J.*, vol. 15, no. 3, pp. 3324–3335, Sep. 2021.

[17] J. Zhang, J. Ye, and L. Guo, “Model-based cyber-attack detection for voltage source converters in island microgrids,” in *Proc. IEEE Energy Convers. Congr. Expo.*, 2021, pp. 1413–1418.

[18] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, “A distributed cyber-attack detection scheme with application to DC microgrids,” *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3800–3815, Sep. 2020.

[19] S. Tan, P. Xie, J. M. Guerrero, J. C. Vasquez, and R. Han, “Cyberattack detection for converter-based distributed DC microgrids: Observer-based approaches,” *IEEE Ind. Electron. Mag.*, vol. 16, no. 3, pp. 67–77, Sep. 2022.

[20] A. Mustafa, B. Poudel, A. Bidram, and H. Modares, “Detection and mitigation of data manipulation attacks in AC microgrids,” *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2588–2603, May 2020.

[21] A. S. Musleh, G. Chen, and Z. Y. Dong, “A survey on the detection algorithms for false data injection attacks in smart grids,” *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[22] M. R. Habibi, S. Sahoo, S. Rivera, T. Dragičević, and F. Blaabjerg, “Decentralized coordinated cyber-attack detection and mitigation strategy in DC microgrids based on artificial neural networks,” *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 4, pp. 4629–4638, Aug. 2021.

[23] M. R. Habibi, H. R. Baghaee, F. Blaabjerg, and T. Dragičević, “Secure control of DC microgrids for instant detection and mitigation of cyber-attacks based on artificial intelligence,” *IEEE Syst. J.*, vol. 16, no. 2, pp. 2580–2591, Jun. 2022.

[24] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, “Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks,” *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5294–5310, Oct. 2021.

[25] X. Fu, M. Niu, and G. Wen, “Detection of stealthy cyber-attack in distributed DC microgrids based on LSTM neural network,” in *Proc. IEEE Int. Conf. Neuromorphic Comput.*, 2021, pp. 8–13.

[26] S. M. Mohiuddin, J. Qi, S. Fung, Y. Huang, and Y. Tang, “Deep learning based multi-label attack detection for distributed control of AC microgrids,” in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids*, 2021, pp. 233–238.

[27] K. Gupta, S. Sahoo, R. Mohanty, B. K. Panigrahi, and F. Blaabjerg, “Distinguishing between cyber attacks and faults in power electronic systems–A non-invasive approach,” *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 11, no. 2, pp. 1578–1588, Apr. 2023.

[28] B. Yang and J. Ye, “Data-driven detection of physical faults and cyber attacks in dual-motor EV powertrains,” in *Proc. IEEE Transp. Electrific. Conf. Expo*, 2022, pp. 991–996.

[29] M. Aucoin, B. Russell, and C. Benner, “High impedance fault detection for industrial power systems,” in *Proc. IEEE Conf. Rec. Ind. Appl. Soc. Annu. Meeting*, 1989, pp. 1788–1792.

[30] J. J. Theron, A. Pal, and A. Varghese, “Tutorial on high impedance fault detection,” in *Proc. IEEE 71st Annu. Conf. Protective Relay Engineers*, 2018, pp. 1–23.

[31] *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources With Associated Electric Power Systems Interfaces*, IEEE Standard 1547-2018 (Revision of IEEE Standard 1547-2003), 2018.

[32] D. G. Photovoltaics and E. Storage, *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources With Associated Electric Power Systems Interfaces*, IEEE Standard 1547-2018, 2018.

[33] B. Mahamedi, M. Eskandari, J. E. Fletcher, and J. Zhu, “Sequence-based control strategy with current limiting for the fault ride-through of inverter-interfaced distributed generators,” *IEEE Trans. Sustain. Energy*, vol. 11, no. 1, pp. 165–174, Jan. 2020.

[34] “Reading onsemi IGBT Datasheets,” [Online]. Available: https://www.onsemi.com/pub/Collateral/AND9068-D.PDF

[35] M. Starke, A. Herron, D. King, and Y. Xue, “Implementation of a publish-subscribe protocol in microgrid islanding and resynchronization with self-discovery,” *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 361–370, Jan. 2019.

[36] S. East, J. Butts, M. Papa, and S. Shenoi, “A taxonomy of attacks on the DNP3 protocol,” in *Proc. Crit. Infrastructure Protection III: 3rd Annu. IFIP WG 11.10 Int. Conf. Crit. Infrastructure Protection*, Hanover, NH, USA, 2009, pp. 67–81.

[37] B. Kang et al., “Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations,” in *Proc. IEEE 20th Conf. Emerg. Technol. Factory Automat.*, 2015, pp. 1–8.

[38] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, “Attack taxonomies for the modbus protocols,” *Int. J. Crit. Infrastructure Protection*, vol. 1, pp. 37–44, 2008.

[39] S. Hochreiter and J. Schmidhuber, “Long short-term memory,” *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.