Distinguishing Between Cyber Attacks and Faults in Power Electronic Systems – A Non-Invasive Approach

Gupta, Kirti; Sahoo, Subham; Mohanty, Rabindra; Panigrahi, Bijaya Ketan; Blaabjerg, Frede

Published in:
IEEE Journal of Emerging and Selected Topics in Power Electronics

DOI (link to publication from Publisher):
10.1109/JESTPE.2022.3221867

Publication date:
2022

Document Version
Accepteret manuscript, peer-review version

Distinguishing Between Cyber Attacks and Faults in Power Electronic Systems – A Non-Invasive Approach

Kirti Gupta, Subham Sahoo, *Member, IEEE,* Rabindra Mohanty, *Member, IEEE,* Bijaya Ketan Panigrahi, *Senior Member, IEEE,* and Frede Blaabjerg, *Fellow, IEEE*

***Abstract*—With increased cyber infrastructure in large power systems with inverter-based resources (IBRs), it remains highly susceptible to cyber attacks. Reliable and secure operations of such system under a large signal disturbance necessitate an anomaly diagnosis scheme, which is substantial for either selective operation of relays (during grid faults), or cybersecurity (during cyber attacks). This becomes a challenge for power electronic systems, as their characteristic response to such large signal disturbance is very fast. Hence, we accumulate our efforts in this paper to characterize between them accurately within a short time frame. A novel non-invasive anomaly diagnosis mechanism for IBRs is presented, which only requires locally measured voltage and frequency as inputs. Mapping these inputs in a X-Y plane, the characterization process is able to classify between the anomalies within 5 ms. To the best of our knowledge, this mechanism provides the fastest decision in comparison to the existing techniques, which also assists the equipped protection/cybersecurity technology to take corresponding decisions without enforcing any customization. The proposed scheme is validated on many systems using real-time (RT) simulations in OPAL-RT environment with HYPERSIM software and also on a hardware prototype. The results verify the effectiveness, scalability and accuracy of the proposed mechanism under different scenarios.**

***Index Terms*—Anomaly diagnosis, cyber-physical system, cyber attacks, faults, inverters.**

I. Introduction

A. Introduction

FUTURE distribution systems will comprise of distributed energy resources (DERs) as its integral part to enhance system reliability and resiliency. Inverter based resources (IBRs) provide a convenient platform to achieve these objectives and manage heterogeneous DERs autonomously. Furthermore, the advancement in computational and communication technologies facilitate in handling the intermittent DERs. In addition, due to the advancements in information and communication technologies (ICT), IBRs follow a standard hierarchical control framework [1], which transforms into a cyber-physical system highly vulnerable to cyber attacks. The recent case study by Recorded Future's Insikt Group revealed that from mid-2020 onwards within India's power sector [2], RedEcho carried out suspected network intrusions, which targeted four out of five Regional Load Dispatch Centres (RLDCs) that are directly responsible for balancing supply and demand in real-time to maintain a stable grid frequency. As a result, power electronic systems security becomes a key driver for protection against such threats.

In the hierarchical layer, distributed framework has come out as a better alternative as compared to the centralized one with enhanced reliability, scalability and cost efficiency. The abovementioned control configuration operates by exchanging information between two neighbouring DERs. Despite enhanced reliability of operation, they can be easily compromised by cyber threats and communication failure. Such anomalies not only restrict the cyber layer but will also compromise the physical layer operation [3]. By definition, an *anomaly* can be described as anything that causes an abnormal behaviour in the system. In IBR based systems, the physical anomalies are shunt faults (both balanced and unbalanced faults) on the bus or line. On the other hand, the cyber attacks can be grouped into cyber anomalies caused by a third-party adversary, accounting illegitimate activities such as data manipulation, data integrity, data delay/loss [4], [5]. Data manipulation attacks are commonly termed as false data injection attacks (FDIAs), which affects the integrity and confidentiality of a system. Whereas, data can also be delayed temporarily or can be lost permanently, commonly termed as denial of service (DoS) attack, due to communication failure or injection of random packets to cause large delay. As the essence of DoS attacks allows it only to be modelled as a large delay, we do not necessarily account this as a cyber anomaly in this paper, as we are investigating the response to large signal disturbances. Hence, we focus on the impact of large signal FDIA on different control layers [6] to differentiate them quickly from system faults.

B. Literature Survey

Recent literature suggests that there are two ways to detect these cyber-physical intrusions in a system: model-based

Kirti Gupta and Bijaya Ketan Panigrahi are with the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi 110016, India (e-mail: {Kirti.Gupta, Bijaya.Ketan.Panigrahi}@ee.iitd.ac.in).

Subham Sahoo and Frede Blaabjerg are with the Department of Energy, Aalborg University, 9220 Aalborg, Denmark (e-mail: {sssa, fbl}@energy.aau.dk).

Rabindra Mohanty is with the Department of Electrical Engineering, Indian Institute of Technology (BHU), Varanasi 221005, India (e-mail: rabindra.eee@iitbhu.ac.in).

This article has supplementary downloadable material available at http://ieeexplore.ieee.org, provided by the authors. The material consists of a multimedia avi format movie clip, which shows the performance of the proposed decentralized cyber-physical anomaly diagnosis mechanism against cyber-physical anomalies for inverter based resources. The size of the movie clip is 17 MB.

and data-driven approaches. In [7] and [8], support vector machine (SVM), decision trees and random forest techniques have been proposed for physical anomaly identification. Further to improve the fault detection accuracy, discrete Fourier and wavelet transforms have been used to pre-process the input data in [9]. An adaptive sliding mode observer based approach was presented in [10] for cyber anomaly detection, assuming complete knowledge of communication topology. Another method based on stochastic linear discrete model-based scheme for FDIA detection without state estimation was proposed in [11]. In [12], a neural network based FDIA detection is proposed. Since these approaches discuss the detection and diagnosis of the cyber and physical anomalies separately, a tailor-made scheme to differentiate them from each other still needs to be explored. It becomes equally crucial as cyber attacks can be deliberately designed having the intrinsic characteristics like a physical fault [13], which will lead to operational failure, if not detected correctly.

Embarking closely on the cyber-physical anomaly diagnosis problem, a data-driven intelligent anomaly identification technique is used to locate and classify between faults and cyber attacks. Although it eliminates complex mathematical modeling, it still requires qualitative data for training pertaining to different fault scenarios. Availability of such qualitative data also limits the design of high accuracy anomaly diagnosis mechanism. In [15], a parametric time frequency logic framework has been presented without any model information. The time-frequency content from the training data is extracted to detect traces of anomaly in testing data. In [16], local frequency and average voltage measurements of standalone inverters in an AC microgrid are mapped into a X-Y plane to differentiate between the cyber-physical anomalies within a margin of 100 ms. As the power electronic protection systems respond within 10 ms (half cycle for a 50 Hz system) [17], the deployment of the abovementioned schemes will remain limited. Hence, a new principle mandates a quick analysis of the prevailing cyber-physical situation in the system and consequently, aid the underlying protection/cybersecurity technology in mitigating the corresponding anomaly.

C. Paper Contributions

To simplify this diagnosis, this paper presents a novel non-invasive technology to characterize between cyber and physical anomalies. It encapsulates physics-informed empirical laws to devise a sample-based trajectory window, where different regions have been formulated for each anomaly. In particular, these regions are mapped in a Δf - ΔV_d plane for each DER. When any movements in these defined regions are detected within a moving window of 5 ms, the corresponding diagnosis will then be formalized. As a result, not only this scheme makes a fast and accurate decision, but also allows the consecutive resilient technologies (protection systems/cybersecurity mechanism) enough time to comprehend the underlying diagnosis. We envision this diagnosis mechanism to be an effective methodology in improving the resiliency of IBRs. We consider large signal FDIAs on frequency and voltage measurements and test the efficacy of the proposed mechanism with several types of faults (such as, LG, LLLG, LL, LLG) on buses and lines of the distribution systems.

Hence, the key contributions of the paper can be summarized as follows:

- We introduce a novel non-invasive anomaly diagnosis scheme to differentiate faults from cyber attacks. We verify our contributions theoretically using physics-informed laws. These laws are then governed online by mapping their trajectories in Δf - ΔV_d plane. Since this diagnosis principle is exploited entirely against locally measured quantities, this makes it a non-invasive approach;
- We also conceptualize additional features in the proposed mechanism, where FDIA attacks (of any scale) on frequency and voltage in an AC power electronics network can be accurately diagnosed within 5 ms. To the best of authors' knowledge, this mechanism provides the fastest decision in comparison to the existing techniques;
- We formalize our findings through a selective and fast decision within 5 ms for any power electronics network, which is engineered based on the minimum tripping time (around 10 ms [17]) during faults;
- We validate our findings by testing its efficacy and scalability in different systems like CIGRE LV and IEEE 37-bus distribution system with certain customization. In addition, it has been highlighted how this mechanism provides accurate decisions even during transient disturbances, cascaded cyber attacks and faults. On the other hand, it also guarantees resiliency against noisy measurements.

The remainder of this paper is organized as: a brief description on modeling and control of IBRs is provided in Section II. The problem behind cyber-physical anomaly diagnosis is explained in Section III. The proposition of the decentralized anomaly diagnosis scheme and its performance validation is presented in Section IV and V, respectively. Finally, we conclude with our remarks and future work in Section VI.

II. Modeling Preliminaries

A. Physical Architecture

To simplify the discussion of modeling and control structure of a networked power electronic system, a 2-bus test setup is considered as an exemplary model in Fig. 1. Each DER comprises of a DC source (e.g., renewable energy or energy storage systems), DC/AC inverter, LC filter and RL output connector [1]. The different types of faults considered in this paper are shown in the Fig. 1 which includes (f1) bus faults and (f2) line faults. These faults can be any of these LG, LLLG, LL or LLG faults with varied fault resistance (R_f) values. The intelligent electronic devices (IEDs) are connected at each end of the line segments to protect the system against any physical faults. In this paper, we consider overcurrent relays (OCRs) as the protection infrastructure. In the physical architecture, i^{th} and j^{th} DER are interconnected to each other via tie-line resistance R_{ij} and reactance X_{ij}. In the primary control layer, there are current and voltage control with a droop controller. Detailed modeling and equations can be referred from [18].

As the secondary controller output directly influences the droop controller entity, we consider further scrutiny here. The droop controller employed in the i^{th} DER to locally regulate frequency and voltage, based on their active power P^i and reactive power, respectively Q^i can be given by:

$$\omega^i(t) = \omega_{ref} - m_p^i P^i(t) \tag{1}$$

$$V_{dref}^i(t) = V_{nom} - n_q^i Q^i(t) \tag{2}$$

where, ω_{ref} and V_{nom} are the desired nominal frequency and voltage, respectively. It is worth notifying that $f = \omega/(2\pi)$ is used, whenever required. The active and reactive power droop coefficients are represented by m_p and n_q, respectively. The relation between instantaneous active (or reactive) power, p (or q) when passed through low-pass filter (ω_c as the cut-off frequency), the active (or reactive) power corresponding to the fundamental component is expressed by:

$$P = \left(\frac{\omega_c}{s+\omega_c}\right) p \quad (3) \qquad Q = \left(\frac{\omega_c}{s+\omega_c}\right) q \quad (4)$$

where, instantaneous active (or reactive power) is represented as:

$$p = 1.5\left(v_d i_d + v_q i_q\right) \tag{5}$$

$$q = 1.5\left(-v_d i_q + v_q i_d\right) \tag{6}$$

As droop controllers do not allow zero steady-state error operation under loaded conditions, secondary controllers are usually employed, where communication becomes intrinsically necessary. Its design and modeling principle is explained in the next subsection.

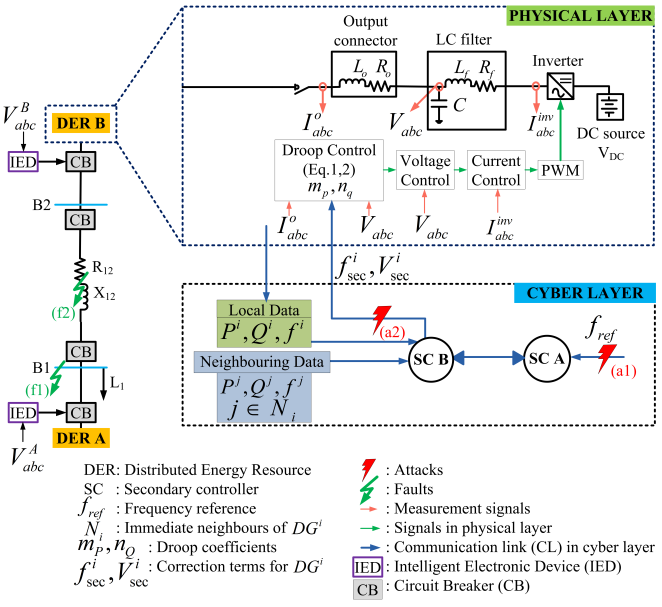

Fig. 1. An exemplary 2-bus cyber-physical system with two DERs, equipped with high-fidelity protection and monitoring systems.

B. Cyber Architecture

As we have discussed in Section I that cooperative coordination is preferred over its centralized counterpart due to its enhanced reliability and stability, we formalize our findings using a cooperative control framework in a system with M DERs in this paper. As shown in Fig. 1, secondary controllers (SCs) communicate among themselves in a sparse cyber network to achieve the desired objectives of frequency restoration, proportionate active and reactive power sharing [19].

Considering each node in the cyber layer as an agent (DER in the physical model) as $\mathbf{x} = \{x_1, x_2, .., x_M\}$ and linked by edges $\mathbf{E}_G$ via an adjacency matrix $\mathbf{A}_G = [a_{ij}] \in R^{M\times M}$. a_{ij} is given as the communication weight from node j to node i. Each agents share information ψ_j = [P^j, Q^j, f^j] with neighbors $N_i = \{j|(x_j, x_i) \in \mathbf{E}_G\}$, where N_i denote the set of neighbors of agent i. The matrix representing incoming information can be given as $\mathbf{D_{in}} = diag\{d_i^{in}\}$, where $d_i^{in} = \sum_{j\in N_i} a_{ij}$. Similarly, the matrix representing outcoming information can be given as $\mathbf{D_{out}} = diag\{d_i^{out}\}$, where $d_i^{out} = \sum_{i\in N_j} a_{ji}$. Then the Laplacian matrix $\mathbf{L} = [l_{ij}]$ can be obtained, given as $\mathbf{L} = \mathbf{D_{in}} - \mathbf{A}_G$. These correction terms are then added to (1) and (2) to get:

$$\omega^i(t) = \omega_{ref} - m_p^i P^i(t) + \omega_{\text{sec}}^i(t) \tag{7}$$

$$V_{dref}^i(t) = V_{nom} - n_q^i Q^i(t) + V_{\text{sec}}^i(t) \tag{8}$$

Neglecting the dynamics of inner control loops, we can assume $V_d^i \approx V_{dref}^i$. Substituting this relationship in (8), we obtain:

$$V_d^i(t) = V_{nom} - n_q^i Q^i(t) + V_{\text{sec}}^i(t) \tag{9}$$

The frequency and voltage error terms designed to be compensated by the secondary controller are e_ω^i and e_v^i, respectively at i^{th} DER. On expanding these error terms, we get:

$$\begin{aligned}\dot{e}_\omega^i(t) = &-\sum_{j\in N_i} a_{ij}\left(m_p^i.P^i(t) - m_p^j.P^j(t)\right) \\ &-\sum_{j\in N_i} a_{ij}\left(\omega^i(t) - \omega^j(t)\right) - g_i\left(\omega^i(t) - \omega_{ref}\right)\end{aligned} \tag{10}$$

$$\dot{e}_v^i(t) = -\sum_{j\in N_i} a_{ij}\left(n_q^i Q^i(t) - n_q^j Q^j(t)\right) \tag{11}$$

$\dot{e}_\omega^i$ and $\dot{e}_v^i$ are then fed into the secondary layer PI controllers G_ω^i and G_V^i, respectively. These PI controllers can be represented as: $G_\omega^i = K_{p\omega}^i + K_{i\omega}^i/s$ and $G_V^i = K_{pv}^i + K_{iv}^i/s$. Finally, the correction signals can be obtained using:

$$\omega_{\text{sec}}^i(t) = K_{p\omega}^i \dot{e}_\omega^i(t) + K_{i\omega}^i e_\omega^i(t) \tag{12}$$

$$V_{\text{sec}}^i(t) = K_{pv}^i \dot{e}_v^i(t) + K_{iv}^i e_v^i(t) \tag{13}$$

Upon combining droop and secondary control signals for frequency control from (7), (12), we get:

$$\omega^i(t) = \omega_{ref} - m_p^i P^i(t) + \underbrace{K_{p\omega}^i \dot{e}_\omega^i(t) + K_{i\omega}^i e_\omega^i(t)}_{\omega_{sec}^i} \tag{14}$$

In a similar manner, combining droop and secondary control signals for voltage control (9), (13) we get:

$$V_d^i(t) = V_{nom} - n_q^i Q^i(t) + \underbrace{K_{pv}^i \dot{e}_v^i(t) + K_{iv}^i e_v^i(t)}_{V_{sec}^i} \quad (15)$$

As evident from (12)-(13), the collaborative nature of the distributed control framework provides a smooth surface for the flow of attack vector from one DER to another. The third-party adversaries can attack any DER or a communication link, which can later circulate throughout the system, thereby affecting the system operation in many ways. As shown in Fig. 1, points of access by an adversary can be: (a1) for reference signals, and (a2) for secondary control command to primary controllers. We consider the large signal frequency and voltage FDIAs for DER i:

$$f_{ref}^{Ci}(t) = f_{ref}^i + \alpha.f_{ref}^{Ai}(t), \quad \alpha = \{0,1\} \quad (16)$$

$$V_{\text{sec}}^{Ci}(t) = V_{\text{sec}}^i(t) + \beta.V_{sec}^{Ai}(t), \quad \beta = \{0,1\} \quad (17)$$

where, α and β being unity, denotes the presence of cyber attack on frequency reference (labeled as (a1) in the Fig. 1) and voltage correction signal (labeled as (a2) in the Fig. 1), respectively. In addition, f_{ref}^{Ai}, V_{sec}^{Ai} are the attack signals on i^{th} DER, deviating the corresponding reference values to f_{ref}^{Ci} and V_{sec}^{Ci}, respectively. Even if the FDIA is conducted on P^i, P^j, Q^i, Q^j, it can be deduced using (12), (13), (10), (11) that the secondary control correction terms will anyway be compromised. Further, the stealth attacks [20] can be easily curated to resemble to that of grid faults. Hence, these attacks need to be immediately removed as soon as they are implanted into the system.

III. Problem Statement

The IBRs are often limited to 1.1-1.5 times of their nominal current rating (I_{rated}) [21], owing to the maximum current capability, prescribed reliability indices and lifetime of the semiconductor switches in each DER. Therefore, conventional overcurrent devices fail to detect and isolate the faulty section in such networks, specifically for low values of fault current. Furthermore, it is difficult to choose overcurrent settings that is both sensitive and selective. One of the straightforward approaches is to increase the fault current contribution by installing over-rated inverters (usually three times the rated current). This method will work effectively with the existing overcurrent relay, but at the cost of higher investment on the inverters [22]. This technique has already been used in a real-world test connecting large battery storage in an islanded LV MG [23]. In this paper, we consider IBRs to be over-rated to three times of the rated current to allow sufficient current for OCR operation.

The peak value of current is continuously monitored by OCR as a combination of active and reactive currents using:

$$I_p = \sqrt{I_d^2 + I_q^2} \quad (18)$$

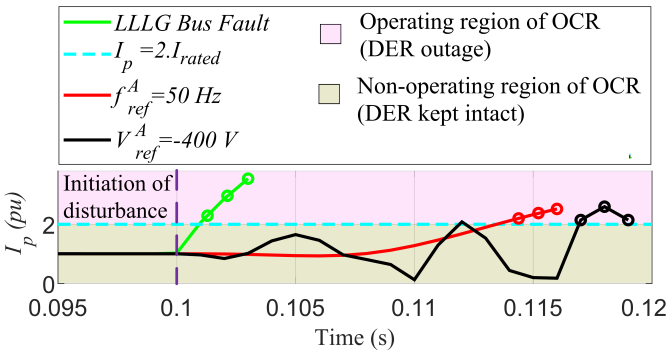

Fig. 2. Time domain simulation of current for a cycle with various cyber-physical anomalies at DER A of a 2-bus test system (Fig. 1).

where, I_p represents the peak value of current, I_d is the active current (d-axis component of peak current) and I_q is the reactive current (q-axis component of peak current). To minimize the voltage drop and to ensure a fast voltage recovery after a fault, each converter limits its reactive current using:

$$I_d = \sqrt{I_{max}^2 - I_q^2} \quad (19)$$

where, I_{max} is the maximum allowable current that prevents inverter from overcurrent damage. A critical disturbance in the system can be checked using the following condition in [24] by continuously monitoring the peak value of current from each converter.

$$||I_p[k] - I_p[k-N]| - |I_p[k-N] - I_p[k-2N]|| \geq 2I_{rated} \quad (20)$$

At a given instant k, a disturbance is detected, only when any three successive samples satisfy the condition in (20), as shown in Fig. 2. The operating region and non-operating region of an overcurrent relay are highlighted in Fig. 2. It can be observed that for all cyber-physical anomalies, including a bus fault or cyber attack on f_{ref} and V_{sec} are capable of triggering the overcurrent relay as three consecutive samples exceeding the threshold value, which eventually leads to a TRIP decision within 20 ms. This would not only cause maloperation of relays during cyber attacks, but also isolate a normally operating DER corresponding to that OCR, thereby affecting the reliability of supply to the consumers.

Hence, this paper proposes a non-invasive method to diagnose and differentiate between cyber attacks and faults as quickly as possible. As mentioned earlier, the deviations in voltage versus deviations in frequency is used as a decisive mechanism in the proposed method to diagnose cyber-physical anomalies in IBRs. In this regard, the design theory of the proposed scheme and its formal proof is elaborated in the following section.

IV. Proposed Anomaly Diagnosis Scheme – Modeling and Formal Guarantees

To design the anomaly diagnosis, it is vital to understand the key differences between faults and cyber attacks. Their difference has been summarized in Table I.

TABLE I
KEY DIFFERENCES BETWEEN PHYSICAL FAULT AND CYBER ATTACK

S.No.	Features	Physical Fault	Cyber Attack
1	Location	Physical layer which include fault on buses or lines.	Cyber layer which include attacks like denial of service (DoS), false data injection (FDI) etc.
2	Physical impact	If not cleared within stipulated time, may cause cascaded failure of equipment and interrupt power supply. This may further cause brownouts (or even blackouts).	Depending on the type of attack, it has different impacts. For instance, DoS attacks affect availability whereas FDIA affects both integrity and confidentiality of signals. FDIA may disguise as fault and may have similar consequences on protection devices as for faults.
3	Impact on the system	Tripping of circuit breakers. A change in Thevenin's equivalent impedance of the system is observed during fault.	May cause tripping of CBs. Cyber attacks do not change the system configuration and thus, the Thevenin's equivalent impedance of the system.

For a three-phase fault, the voltage and current can be expressed as

$$v_f(t) = R_{eq} i_f(t) + L_{eq} \frac{di_f(t)}{dt} \tag{21}$$

$$i_f(t) = \frac{V_m}{|Z|} \left[\sin(\omega t + \theta - \alpha) - e^{-\frac{R_{eq} t}{L_{eq}}} \sin(\theta - \alpha) \right] \tag{22}$$

where, $v_f(t)$ and $i_f(t)$ are the voltage and current during fault, t is the fault inception time. The equivalent resistance and impedance in the faulted loop is represented by R_{eq} and L_{eq} respectively. $|Z| = \sqrt{R_{eq}^2 + (\omega L_{eq})^2}$ and $\alpha = \tan^{-1}\left(\frac{\omega L_{eq}}{R_{eq}}\right)$. From (21) and (22), it is clear that changes in both voltage and current during fault depend on the system parameters, thus is an inherent function of system dynamics. Differently from faults, cyber attacks in (16)-(17) will have different behavior, which is highly dependent on the overall system loading condition, and will always implicit the secondary controller dynamics as they are introduced as disturbances in that loop. This can be justified using the theoretical analysis below, which has been conducted for R and RL loading conditions.

In Fig. 1, the voltages at bus B2 can be given by:

$$V_i \angle \alpha_i = E_i \angle \delta_i - (r_i + j x_i) I_i \angle - \theta_i \tag{23}$$

where, $I_i \angle - \theta_i$ is the output current of the i^{th} DER. Using (1)-(2), we can further obtain:

$$V_i = E_i^* - n_q Q_i - r_i I_i \cos\gamma_i - x_i I_i \sin\gamma_i \tag{24}$$

where, $\gamma_i = \alpha_i + \theta_i$. Finally, to compensate for the error caused by the line drop and to acquire equal reactive power sharing, we introduce a cooperative secondary controller term V_{sec}^i using:

$$V_{sec}^i(t) = K_{pv}^i \dot{e}_v^i(t) + K_{iv}^i e_v^i(t) \tag{25}$$

where, $\dot{e}_v^i(t) = -\sum_{j \in N_i} a_{ij} \left(n_q^i Q^i(t) - n_q^j Q^j(t) \right)$ is the error between reactive power droop terms of local and neighboring DGs. Finally, adding (25) in (24) and segregating the control terms to the RHS, we get:

$$V_i + r_i I_i \cos\gamma_i + x_i I_i \sin\gamma_i = E_i^* - n_q Q_i + V_{sec}^i \tag{26}$$

Since the reactive power drop and inductive load at bus B1 administers the total reactive power generation from bus B2 and assuming line drop to be negligible, we can equalize the reactive power generation from bus B2 to be approximately equal to the reactive power demand Q_d, we get:

$$\underbrace{V_i + r_i I_i \cos\gamma_i + x_i I_i \sin\gamma_i}_{V_i^*} + n_q Q_i = E_i^* + V_{sec}^i \tag{27}$$

$$V_i^* [1 + \frac{V_i^*}{X_d}] = E_i^* + V_{sec}^i \tag{28}$$

When we augment the model for voltage based cyber attacks given by:

$$V_{\text{sec}}^{Ci}(t) = V_{\text{sec}}^i(t) + \beta . V_{sec}^{Ai}(t), \qquad \beta = \{0, 1\} \tag{29}$$

into (28), we get:

$$V_i^* [1 + \frac{V_i^*}{X_d}] = E_i^* + V_{sec}^{Ci} \tag{30}$$

Using (30), we can conclude that for any values of V_{sec}^{Ci}, the trajectory movement for voltage with respect to frequency will always be positive since all the terms in LHS are positive as long as there are no faults (where V_i will drop down). Finally, when there are only R loads instead of RL loads, Q_d = 0. As a result, the voltage change is regulated in proportion with the active power demand and can be associated with change in γ_i as per (1), which can then traverse into the negative region in the proposed trajectory monitor.

The significance of anomaly diagnosis is presented in Fig. 3 to certify the relevance of the proposed mechanism in addressing the problem. Considering a typical operation time of commercial OCRs to be around 20 ms (in a 50 Hz system) [25], the proposed diagnosis scheme provides a solution by investigating the trajectory of $\Delta f(pu)$ and $\Delta V_d(pu)$ within 5 ms (20 samples/cycle) window, to have a selective and fast decision such that the protection system remains unaltered. As the permissible limits of frequency deviation is commonly around $\pm$ 1% and that of voltage deviation is $\pm$ 5% from the rated value [26], the trajectory as per the proposed method lies within these allowable limits, as shown in Fig. 3. The origin (O) is at (0,0). It is worth notifying that the operating frequency is denoted by f_{ref} in Fig. 5.

For a sampling frequency of 1 kHz, the deviations of frequency and d-axis voltage from the instant of disturbance (considering k^{th} time instant) detected from (20) can be expressed by:

$$\Delta f^i(k) = f^i(k) - f^{i_{pre}} \tag{31}$$

$$\Delta V_d^i(k) = V_d^i(k) - V_d^{i_{pre}} \tag{32}$$

TABLE II
ANOMALY CHARACTERISTICS FOR EVENTS AT DER^i.

Events	Parameters	Δf^i (pu)	ΔV_d^i (pu)	Initial Traversal
Normal/Loading	ΔV_d^i, Δf^i within allowable range	Within ± 0.01	Within ± 0.05	Within permissible V and f ranges
Fault	$\Delta V_d^i < -0.05$ pu	Within ± 0.01	< -0.05	Along negative V_d axis covering Q III, Q IV
Frequency-based cyber attack	f_{ref}^{Ci}=$f_{ref}^{i} + f_{ref}^{Ai}$	$f_{ref}^{C} > f_{ref}$	Within ± 0.05	Along positive Δf axis
		$f_{ref}^{C} < f_{ref}$	Within ± 0.05	Along negative Δf axis
Voltage-based cyber attack	V_{sec}^{Ci}=V_{sec}^{i}+V_{sec}^{Ai}	Within ± 0.01	> 0.05	Along positive V_d axis covering Q I, Q II

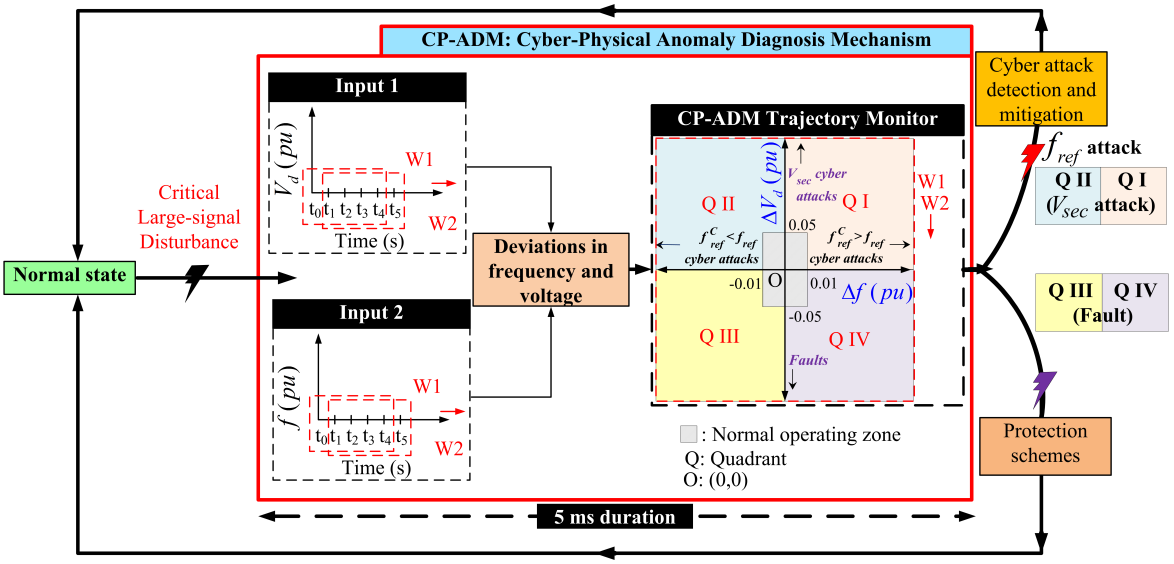

Fig. 3. Cyber-physical anomaly diagnosis mechanism (CP-ADM) for IBRs.

where, $f^{i_{pre}}$ and $V_d^{i_{pre}}$ are buffer data of frequency and voltage measurements for 5 ms window stored as pre-disturbance values, which are constantly updated. The frequency and voltage at each instant can be calculated using (14) and (15), respectively. Finally using Table II, the cyber-physical anomalous regions are classified. For any physical anomaly (like bus/line faults), trajectory movement is along the negative ΔV_d axis with a frequency deviation between $\pm$ 1% (in Quadrants III and IV) whereas, for voltage based cyber attacks, the initial traversal is along the positive ΔV_d axis with a frequency deviation between $\pm$ 1% (in Quadrants I and II). This distinguishes the physical faults from voltage-based cyber attacks. Further, for cyber attacks on the f_{ref} signal, the trajectory moves on either sides of ΔV_d axis depending on the sign of f_{ref}^A with a voltage deviation between $\pm$ 5%. For positive sign of f_{ref}^A, the trajectory moves to the positive side of Δf axis (i,e, towards right) and vice-versa. To demonstrate its efficacy and scalability, the proposed scheme has been tested on a real-time platform on two case studies in OPAL-RT environment. This has been proved to be effective for various scenarios of faults, cyber attacks, loading conditions, simultaneous occurrence of cyber-physical events and addition of noise in the measured data (input to the proposed anomaly diagnosis scheme). All the abovementioned scenarios have been discussed in detail in the next section.

V. PERFORMANCE EVALUATION

The performance of the proposed method is tested on two benchmark distribution systems, CIGRE LV distribution system and IEEE 37-bus distribution systems. These systems were modified to incorporate the inverter-interfaced DERs to operate in an islanded mode where the nominal voltage level of these systems being 400 V and 381 V, respectively. In addition, the nominal frequency f_{ref} is equal to 50 Hz for both systems. To prove the robustness of the proposed scheme, it has been tested under multiple scenarios:

- physical anomalies (like LLLG, LG, LLG, LL faults) on buses as well as in between lines;
- effect of fault resistance (R_f) during physical anomalies;
- effect of load variations;
- cyber anomalies like frequency and voltage based attacks considered one at a time, on individual DERs ;
- simultaneous cyber attacks on multiple DERs;
- the measured data (input to the proposed scheme) was mixed with noise signal to obtain signal to noise ratio (SNR) of 30 dB and 40 dB.

A. Response to faults and cyber attacks in the modified CIGRE LV benchmark system

The standard CIGRE LV distribution system was modified by adding five inverters at buses B6, B10, B18, B16 and B15 as shown in Fig. 4.

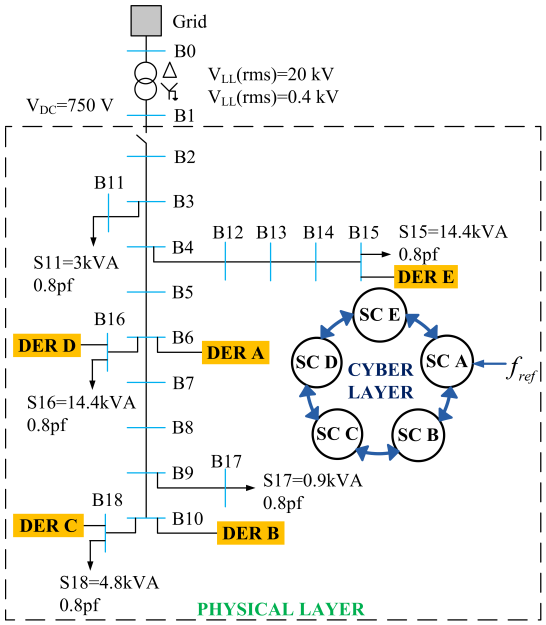

Fig. 4. Modified CIGRE LV islanded distribution system (in dashed section).

Operating with a fixed switching frequency f_s = 10 kHz, the apparent power S of the loads along with their power factor are highlighted in Fig. 4. The line and load parameters of the benchmark system can be obtained from [27] assuming fixed DC sources with balanced loads. To evaluate the performance of the proposed scheme, inverter-interfaced systems have been simulated in real-time in OP-5700 with HYPERSIM software as shown in the testbed in Fig. 5. The physical and cyber layer of DER is modeled in HYPERSIM and RT simulation is carried out through OP 5700. Further, SEL-3530 RTAC serves two purposes of generating frequency reference signal and monitoring the signals like voltage, power, frequency through human machine interface (HMI) . The sampled value protocol is incorporated for distributed secondary control and DNP3 is integrated to generate frequency reference signal and monitor the signals in a microgrid. The equations as discussed in Section II for primary and secondary controllers are presented in Fig. 5. The detailed description of the testbed can be referred from [28]. The control parameters corresponding to primary and secondary control of DERs in modified CIGRE LV islanded distribution system are mentioned in Table. III. The proportional gains of voltage and current control are denoted as K_{pe} and K_{pc} respectively. Further, integral gains of voltage and current control are denoted as K_{ie} and K_{ic} respectively.

The DER A in this system is selected to be the target of cyber-physical anomalies. The response of deviations in d-axis voltage with respect to deviations in frequency for DER A is illustrated in Fig. 6, for a 5 ms cycle window. During normal conditions, the trajectory would lie within the permissible limits around the origin.

TABLE III
CONTROL PARAMETERS OF DERS IN MODIFIED CIGRE LV SYSTEM IN FIG. 4

Droop coefficients	m_p	9.4 x 10^{-5} rad/(Ws)
	n_q	1.3 x 10^{-3} V/VAr
Compensator Gains	K_{pe}	0.1
	K_{ie}	0.5
	K_{pc}	40
	K_{ic}	80
	$K_{i\omega}$	25
	K_{iv}	0.5
Reference frequency	ω_{ref}	314.15 rad/s

To illustrate various anomalous situations in a simple way, plots for frequency-based attacks are not zoomed in. However, as trajectories for voltage-based cyber attacks and faults are on either side of ΔV_d axis, these regions are zoomed in to illustrate the follow through into the quadrants. The time-scale separation between the primary and secondary controllers differs by considerably large values (approximately 10 times), it can consequently aid in differentiating between the cyber-physical anomalies.

B. Responses for the modified IEEE 37-bus distribution system

The standard IEEE 37-bus system was also modified by adding seven inverters at buses B 15, B 18, B 22, B 24, B 29, B 33, and B 34 as shown in Fig. 7. The inverter control parameters are tabulated in Table. IV. For the purpose of brevity,the network and load parameters can be referred from [29].

TABLE IV
CONTROL PARAMETERS OF DERS FOR MODIFIED IEEE-37 BUS SYSTEM IN FIG. 7

Droop coefficients	m_p	9.4 x 10^{-5} rad/(W.s)
	n_q	1.3 x 10^{-3} V/VAr
Compensator gains	K_{pe}	0.2
	K_{ie}	1
	K_{pc}	50
	K_{ic}	100
	$K_{i\omega}$	42
	K_{iv}	1.5
Reference frequency	ω_{ref}	314.15 rad/s

In Fig. 8, the efficacy of the proposed diagnosis certificates in the trajectory monitor is tested for faults at different locations. In this scenario, we consider bus fault at B15 and a line fault between B14 and B15 to check if the trajectory monitor provides any distinctive performance. However, the trajectories provide nearly accurate response for different kinds of faults, which is diagnosed by DER A in an unbiased fashion. In this case, the effect of line impedance during faults is apparent for faults with high resistance. However, the proposed diagnosis anyway remains valid as the trajectory movement is always inclined in the defined regions in Table II.

Furthermore, an effective response to various loading conditions like increment and decrement of load resistances R_L and reactances X_L by a factor represented by s% individually was tested and verified. As shown in Fig. 10,

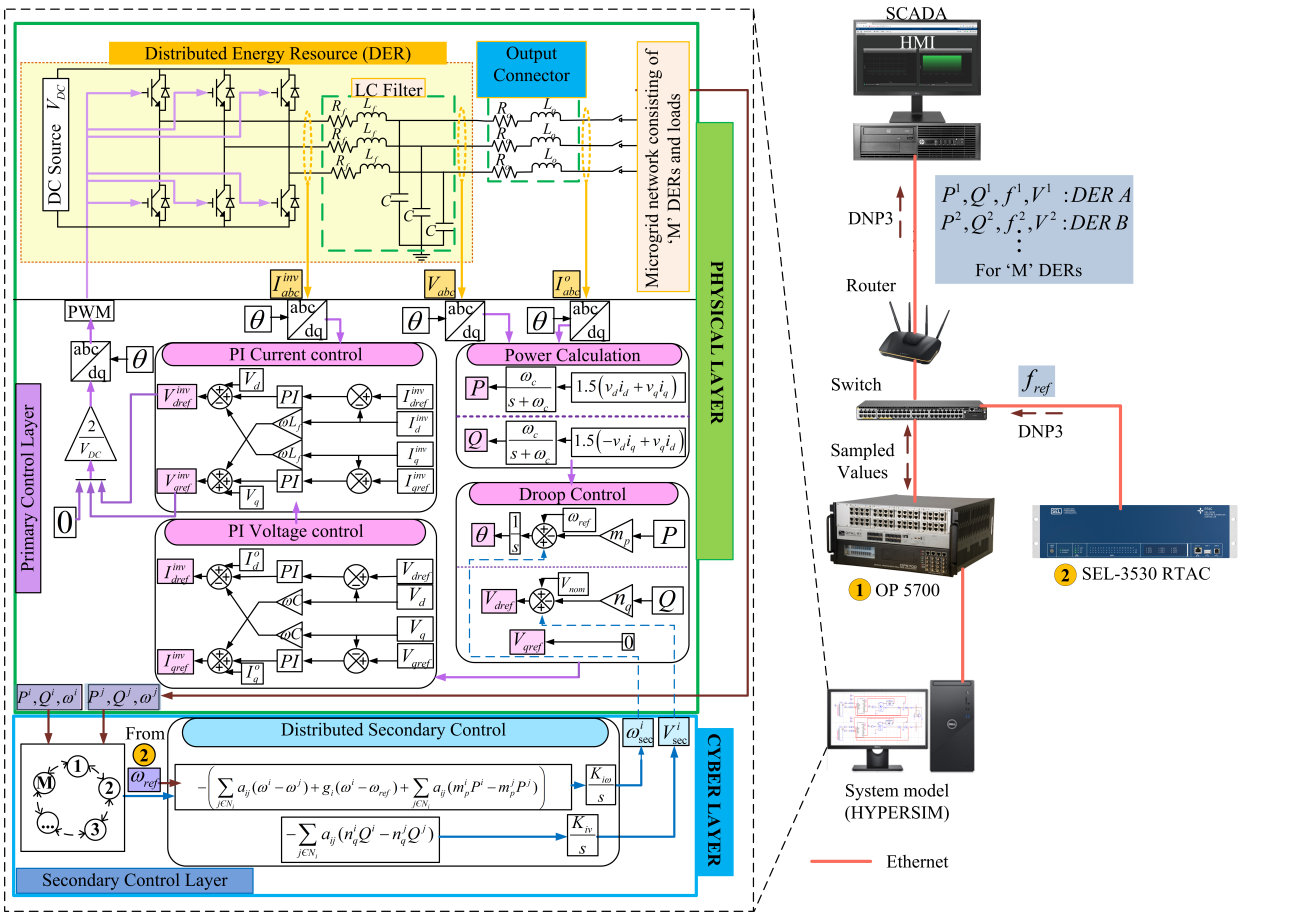

Fig. 5. Testbed for real-time simulation [28] to evaluate the performance of the proposed scheme – the modeling and control schematic of one DER interacting with the cyber layer is highlighted. This DER model can be integrated into the benchmark systems in Fig. 7 and 10.

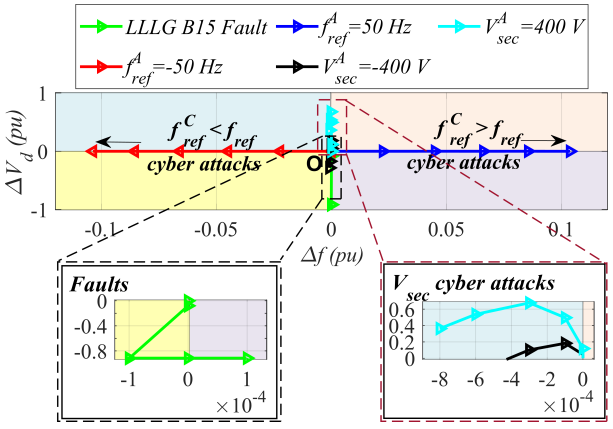

Fig. 6. Trajectories captured for voltage and frequency deviation at DER A for modified CIGRE LV distribution system within 5 ms.

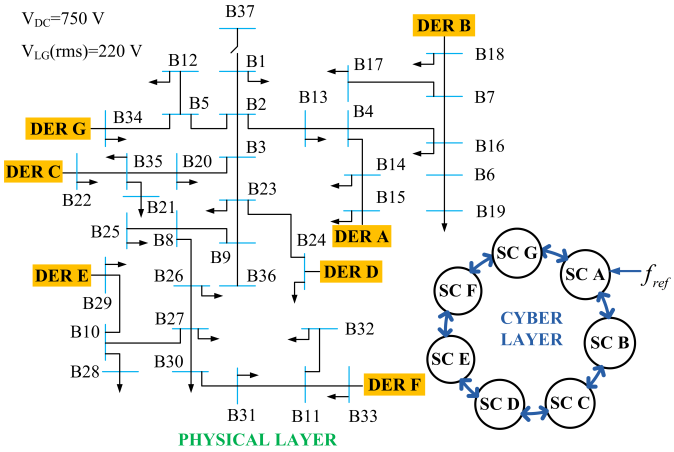

Fig. 7. Modified IEEE 37-bus islanded distribution system.

the load is varied by 10% at B15 (denoted as L15). In particular, the load at B15 is halved and then doubled to its original value. As per the proposed non-invasive method, the trajectories anyway lie within the normal operating region/boundaries, which can be seen in Fig. 10 and Fig. 11 .

In addition, simultaneous cyber attacks across different buses is also simulated to verify the efficacy of the proposed approach in affected buses. For V_{sec} attack at DER A and LLLG fault between B11 and B33 (close to DER F), it can be seen in Fig. 12 that the proposed mechanism characterizes and localizes the anomaly as per the designated regions in Table II. It can be followed that the faulted trajectory moves along the negative Y axis, unleashing within Q III and Q IV.

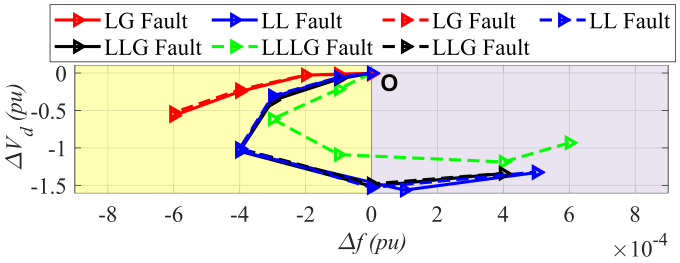

Fig. 8. Trajectories of voltage and frequency deviation at DER A for bus fault at B15 (solid lines) and line fault between B14 and B15 (dashed lines) for modified IEEE 37-bus distribution system for W1 at DER A in Fig. 7.

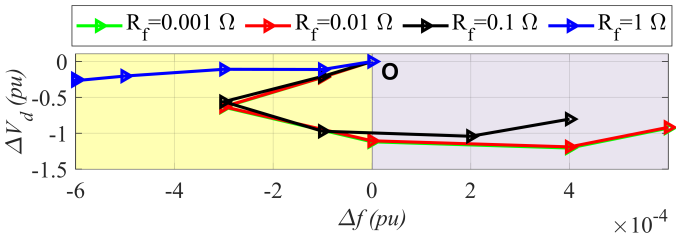

Fig. 9. Trajectories of voltage and frequency deviation at DER A for LLLG fault at B 15 with different R_f for modified IEEE 37-bus distribution system for W1 in Fig. 7.

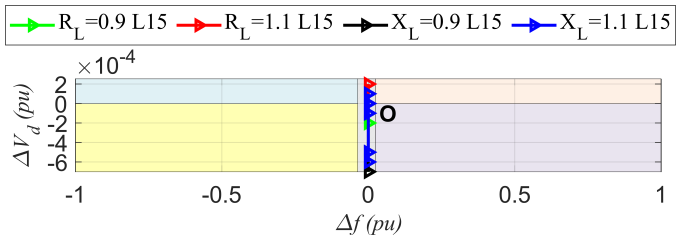

Fig. 10. Trajectories of voltage and frequency deviation at DER A at different loading conditions for modified IEEE 37-bus distribution system for W1 in Fig. 7.

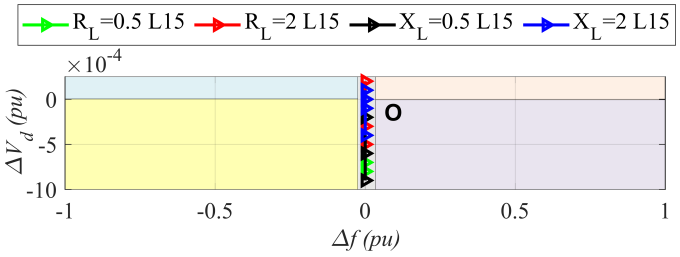

Fig. 11. Trajectories of voltage and frequency deviation at DER A at different loading conditions for modified IEEE 37-bus distribution system for W1 in Fig. 7.

However for voltage based cyber attacks, the trajectories move into positive V_d axis covering Q I and Q II validating the proposed diagnosis mechanism.

Finally, the proposed scheme was tested with noisy measurements having a SNR around 30 dB. This test was performed with the addition of white gaussian noise into V_d and f signals. Regardless of the noise, it can be seen in Fig. 13 that the scheme performs well even under distorted data, as it can successfully diagnose between the cyber and physical anomalies.

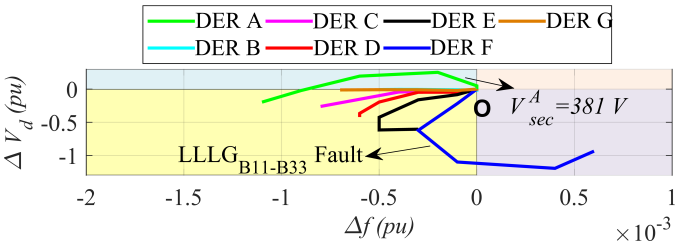

Fig. 12. Trajectories of voltage and frequency deviation at DER A with V_{sec} attack at DER A and LLLG fault between B11 and B33 for modified IEEE 37-bus distribution system for W1 in Fig. 7.

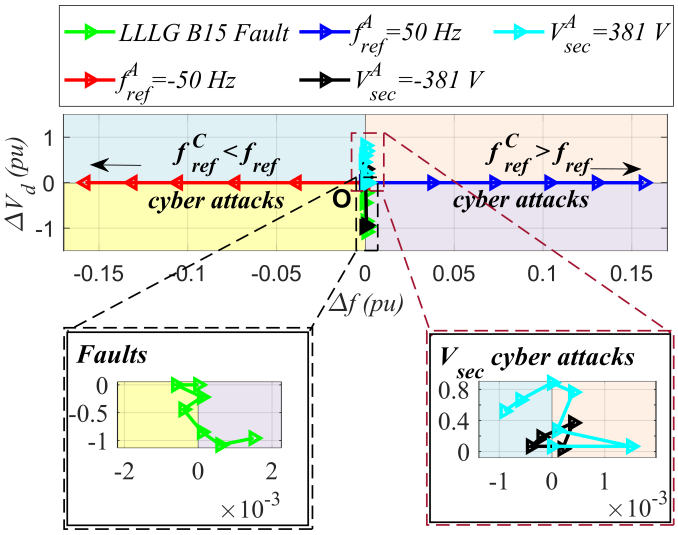

Fig. 13. Trajectories of voltage and frequency deviation at DER A with SNR of 30 dB for modified IEEE 37-bus distribution system for W1 in Fig. 7.

To validate the practicality and rugged performance of the proposed method, experimental tests have been conducted according to the system in Fig. 1. The experimental setup is shown in Fig. 14. Two racks with three-phase 7-kW DC-AC converters are modeled as DER A and B. Finally, there are interconnected to each other through LC filters, circuit breakers and transmission line to a programmable PQ load. The key parameters are listed in Appendix.

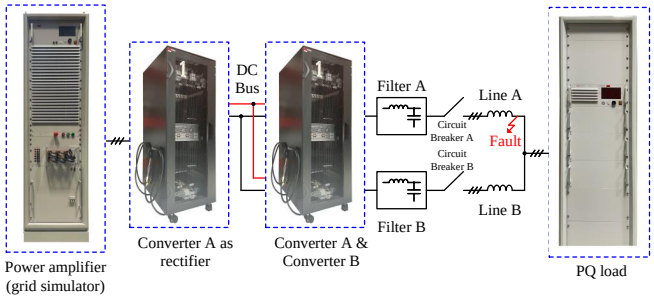

Fig. 14. Experimental prototype of the system topology in Fig. 1.

It is worth notifying that the fault and cyber attack disturbances in Fig. 15 were allowed to persist for a considerable

TABLE V
COMPARATIVE EVALUATION OF THE PROPOSED ANOMALY DIAGNOSIS MECHANISM FOR IBRS.

Features	[14]	[15]	[16]	**Proposed scheme**
Computational burden	High	High	Low	Low
Additional resources	Training data	Training data	✗	✗
Classification of anomalies	✓	✓	✓	✓
Localization of anomalies	✓	✗	Not tested	✓
Decentralized approach	✗	✗	✓	✓
Detection time	Not specified	Not specified	100 ms	5 ms
Effective during transient disturbances (load changes)	Not tested	Not tested	Not tested	✓
Effective during simultaneous attack and fault events	Not tested	Not tested	Not tested	✓
Resilient against distorted measurement data	✓	✓	Not tested	✓

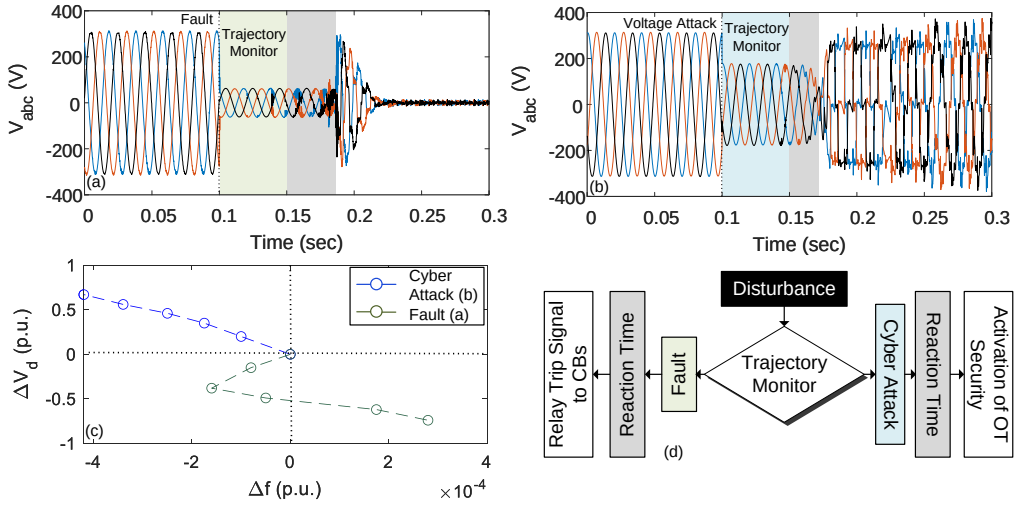

Fig. 15. (a) Voltage of DER A during emulated fault, (b) voltage of DER A during cyber attack in the experimental prototype – a buffer time of 0.05 sec was given for the decision by the trajectory monitor in (c) for a sampling frequency of 100 Hz for the relay signals. Finally, a decision schematic has been shown in (d) to distinguish between cyber attacks and faults using the proposed trajectory monitor and the corresponding action in each case.

time, such that the practicality can be understood easily. In real-time conditions, the reaction time of relays/cybersecurity technologies and sampling frequency of relay measurements will be faster. When the corresponding disturbance is initiated at t = 0.1 sec, it can be seen in Fig. 15(a) that the voltage collapses to a small value following an attack. Similarly, the voltage of DER A collapses during a cyber attack as per its magnitude in Fig. 15(b). As per the proposed strategy, the deviations in V_d w.r.t. f of DER A are monitored in Fig. 15(c) to diagnose between the anomalies. It should be noted that the proposed trajectory monitor is run in parallel with the operation of DER A during the anomalies in Fig. 15(a) & (b). Based on the established anomaly diagnosis certificates, it duly matches the performance as per the results obtained in real-time simulations with PQ loads in the system. Furthermore, as the decision is bypassed to the protection scheme for faults in Fig. 15(a), the circuit breaker A trips DER A out of the system. However, for the cyber attack in Fig. 15(b), the decision is routed to the cyber attack mitigation scheme [16], which allows the system to restore back its operation to the normal voltage levels.

A comparative assessment of the proposed non-invasive cyber-physical anomaly diagnosis mechanism for IBRs is carried out in Table V as opposed to the existing schemes [14]–[16]. It is evident from Table V that the proposed scheme has the potential of becoming a commercial solution as it allows a non-invasive approach to detect and distinguish between cyber and physical anomalies within 5 ms without enforcing high computational burden and additional resources for its design. Its capability of diagnosis within 5 ms also provides a qualitative advantage for the deployment into the existing infrastructures. Moreover to realize its feasibility of operation in an industrial environment with noisy measurements, the proposed scheme also offers resiliency against such distorted measurements.

VI. CONCLUSION AND FUTURE SCOPE OF WORK

In this work, a non-invasive cyber-physical anomaly diagnosis mechanism based on physics-informed empirical laws

has been proposed. It successfully distinguishes between various cyber and physical anomalies in a cyber-physical power electronic system. The proposed technique uses a sample-based trajectory, wherein for each cyber and physical anomaly, different identification regions have been formulated. This approach has an edge over the existing techniques as it distinguishes anomalies within 5 ms using local measurements at a sampling frequency of 1 kHz. To our best knowledge, this is the fastest diagnosis time that has been reported to address this problem. Its testing has been carried out under various cyber-physical anomalies occurring on individual/multiple DERs simultaneously. The experiments have been carried out on a real-time digital simulator OPAL-RT with HYPERSIM for customized two benchmark systems: CIGRE LV benchmark system and IEEE 37-bus distribution system and an experimental prototype of a 2 bus system. Its capability of diagnosis within 5 ms also provides a qualitative advantage for the deployment into the existing infrastructures.

As a future scope of work, we aim to calibrate this algorithm into any system with non-linear loads, which can provide a generalized trajectory region to distinguish between the considered cyber-physical anomalies.

APPENDIX

Two three-phase grid-tied converters (DER A & B) of 7.5 kVA are connected to the programmable PQ load via interfacing LC filters, filter A and B. It should be noted that all the control parameters are consistent for both converters. **System:** L_f= 1.5 mH, C_v = 10 μF,V_n = 230 V/50 Hz, Voltage loop gains: K_{pv} = 0.04, K_{iv} = 168, Current loop gains: K_{pi} = 10.5, K_{iv} = 16000, m_p = 4.8 x 10^{-5} rad/(Ws), n_q = 1.3 x 10^{-3} V/VAr, K_{pe}= 0.07, K_{ie} = 0.4, K_{pc} = 2, K_{ic} = 22.4, $K_{i\omega}$ = 2.8, K_{iv} = 0.36.

REFERENCES

[1] D. Y. Yassuda, I. Vechiu, and J. P. Gaubert, "A review of hierarchical control for building microgrids," *Renew. and Sustain. Ener. Rev.*, vol. 118, pp. 109253, 2020.

[2] https://www.recordedfuture.com/redecho-targeting-indian-power-sector/ (accessed November 2021).

[3] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber Security in Control of Grid-Tied Power Electronic Converters–Challenges and Vulnerabilities," *IEEE J. Emerg. Sel. Topics Power Electron.*, doi: 10.1109/JESTPE.2019.2953480.

[4] J. Duan and M. Chow, "A Novel Data Integrity Attack on Consensus-Based Distributed Energy Management Algorithm Using Local Information," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1544-1553, March 2019, doi: 10.1109/TII.2018.2851248.

[5] C. Deng, F. Guo, C. Wen, D. Yue, and Y. Wang, "Distributed Resilient Secondary Control for DC Microgrids Against Heterogeneous Communication Delays and DoS Attacks," *IEEE Trans. Ind. Electron.*, doi: 10.1109/TIE.2021.3120492.

[6] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A Cyber-Attack Resilient Distributed Control Strategy in Islanded Microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3690-3701, Sept. 2020, doi: 10.1109/TSG.2020.2979160.

[7] S. Kar, S. R. Samantaray, and M. D. Zadeh, "Data-Mining Model Based Intelligent Differential Microgrid Protection Scheme," *IEEE Syst. J.*, vol. 11, no. 2, pp. 1161-1169, June 2017, doi: 10.1109/JSYST.2014.2380432.

[8] E. Casagrande, W. L. Woon, H. H. Zeineldin, and D. Svetinovic, "A Differential Sequence Component Protection Scheme for Microgrids With Inverter-Based Distributed Generators," *IEEE Trans. Smart Grid*, vol. 5, no. 1, pp. 29-37, Jan. 2014, doi: 10.1109/TSG.2013.2251017.

[9] S. C. Paiva, R. L. de Araujo Ribeiro, D. K. Alves, F. B. Costa, and T. d. O. A. Rocha, "A wavelet-based hybrid islanding detection system applied for distributed generators interconnected to AC microgrids," *Int. J. Elect. Power & Energy Sys.*, vol. 121, p. 106032, 2020.

[10] W. Ao, Y. Song, and C. Wen, "Adaptive cyber-physical system attack detection and reconstruction with application to power systems," *IET Control Theory & Appl.*, vol. 10, no. 12, pp. 1458-1468, 2016.

[11] Z. Pang, G. Liu, D. Zhou, F. Hou, and D. Sun, "Two-Channel False Data Injection Attacks Against Output Tracking Control of Networked Systems," *IEEE Trans. Ind. Electron.*, vol. 63, no. 5, pp. 3242-3251, May 2016, doi: 10.1109/TIE.2016.2535119.

[12] A. Abbaspour, A. Sargolzaei, P. Forouzannezhad, K. K. Yen, and A. I. Sarwat, "Resilient Control Design for Load Frequency Control System Under False Data Injection Attacks," *IEEE Trans. Ind. Electron.*, vol. 67, no. 9, pp. 7951-7962, Sept. 2020, doi: 10.1109/TIE.2019.2944091.

[13] M. A. Khan, V. S. Bharath Kurukuru, S. Sahoo and F. Blaabjerg, "From Physics to Data Oriented Cyber Attack Profile Emulation in Grid Connected PV Systems," *2021 IEEE 22nd Workshop on Control and Modelling of Power Electronics (COMPEL)*, pp. 1-8, 2021.

[14] A. A. Khan, O. A. Beg, M. Alamaniotis, and S. Ahmed, "Intelligent anomaly identification in cyber-physical inverter-based systems," *Electric Power Systems Research*, vol. 193, p. 107024, 2021.

[15] O. A. Beg, L. V. Nguyen, T. T. Johnson and A. Davoudi, "Cyber-Physical Anomaly Detection in Microgrids Using Time-Frequency Logic Formalism," *IEEE Access*, vol. 9, pp. 20012-20021, 2021, doi: 10.1109/ACCESS.2021.3055229.

[16] S. Sahoo, Y. Yang, and F. Blaabjerg, "Resilient Synchronization Strategy for AC Microgrids Under Cyber Attacks," *IEEE Trans. Power Electron.*, vol. 36, no. 1, pp. 73-77, Jan. 2021, doi: 10.1109/TPEL.2020.3005208.

[17] A. Chattopadhyay, A. Ukil, D. Jap and S. Bhasin, "Toward Threat of Implementation Attacks on Substation Security: Case Study on Fault Detection and Isolation," *IEEE Trans. Ind. Inform.*, vol. 14, no. 6, pp. 2442-2451, June 2018, doi: 10.1109/TII.2017.2770096.

[18] N. Pogaku, M. Prodanovic, and T. C. Green, "Modeling, Analysis and Testing of Autonomous Operation of an Inverter-Based Microgrid," *IEEE Trans. Power Electron.*, vol. 22, no. 2, pp. 613-625, March 2007, doi: 10.1109/TPEL.2006.890003.

[19] M. Raeispour, H. Atrianfar, H. R. Baghaee, and G. B. Gharehpetian, "Resilient H∞ Consensus-Based Control of Autonomous AC Microgrids With Uncertain Time-Delayed Communications," in *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3871-3884, Sept. 2020, doi: 10.1109/TSG.2020.2992646.

[20] S. Sahoo, S. Mishra, J. C. -H. Peng and T. Dragičević, "A Stealth Cyber-Attack Detection Strategy for DC Microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162-8174, Aug. 2019.

[21] M. J. Reno, S. Brahma, A. Bidram, and M. E. Ropp, "Influence of Inverter-Based Resources on Microgrid Protection: Part 1: Microgrids in Radial Distribution Systems," IEEE Power and Energy Mag., vol. 19, no. 3, pp. 36-46, May-June 2021, doi: 10.1109/MPE.2021.3057951.

[22] A. Burstein, V. Cuk, and E. de Jong, "Effect of network protection requirements on the design of a flexible AC/DC-link," *J. Eng.*, vol. 2018, no. 15, pp. 1291–1296, 2018.

[23] F. Van Overbeeke, W. Bos, R. Verzijbergh, et al. "Advanced architectures and control concepts for MORE MICROGRIDS: final report task TF5". 2010. [Online]. Available: http://www.microgrids.eu (accessed November 2021)

[24] A. Jalilian, M. T. Hagh, and S. M. Hashemi, "An Innovative Directional Relaying Scheme Based on Postfault Current," IEEE Trans. Power Del., vol. 29, no. 6, pp. 2640-2647, Dec. 2014, doi: 10.1109/TPWRD.2014.2312019.

[25] J. L. Blackburn and T. J. Domin, Protective relaying: principles and applications. CRC press, 2006.

[26] O. Mohammed, T. Youssef, M. H. Cintuglu, and A. Elsayed, "Design and simulation issues for secure power networks as resilient smart grid infrastructure," *Smart Energy Grid Engineering*. Amsterdam, The Netherlands: Elsevier, pp. 245–342, 2017.

[27] S. Barsali, Benchmark systems for network integration of renewable and distributed energy resources. 2014.

[28] K. Gupta, S. Sahoo, B. K. Panigrahi, F. Blaabjerg, and P. Popovski, "On the Assessment of Cyber Risks and Attack Surfaces in a Real-Time Co-Simulation Cybersecurity Testbed for Inverter-Based Microgrids," *Energies*, vol. 14, no. 16, p. 4941, 2021.

[29] L. Luo and S. V. Dhople, "Spatiotemporal model reduction of inverter-based islanded microgrids," *IEEE Trans. Energy Convers.*, vol. 29, no. 4, pp. 823–832, Dec. 2014.