Cyber-Resilient Fault Diagnosis Methodology in Inverter-Based Resource-Dominated Microgrids with Single-Point Measurement

Yifan Wang
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore, Singapore
wang2115@e.ntu.edu.sg

Yiyao Yu
College of Design and Engineering
National University of Singapore
Singapore, Singapore
e1350878@u.nus.edu

Yang Xia
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore, Singapore
yang_xia@ntu.edu.sg

Yan Xu
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore, Singapore
xuyan@ntu.edu.sg

***Abstract*—Cyber-attacks jeopardize the safe operation of inverter-based resource-dominated microgrids (IBR-dominated microgrids). At the same time, existing diagnostic methods either depend on expensive multi-point instrumentation or stringent modeling assumptions that are untenable under single-point measurement constraints. This paper proposes a Fractional-Order Memory-Enhanced Attack-Diagnosis Scheme (FO-MADS) that achieves timely fault localization and cyber-resilient fault diagnosis using only one VPQ (voltage, active power, reactive power) measurement point. FO-MADS first constructs a dual fractional-order feature library by jointly applying Caputo and Grünwald-Letnikov derivatives, thereby amplifying micro-perturbations and slow drifts in the VPQ signal. A two-stage hierarchical classifier then pinpoints the affected inverter and isolates the faulty IGBT switch, effectively alleviating class imbalance. Robustness is further strengthened through Progressive Memory-Replay Adversarial Training (PMR-AT), whose attack-aware loss is dynamically re-weighted via Online Hard Example Mining (OHEM) to prioritize the most challenging samples.**

Experiments on a four-inverter IBR-dominated microgrid testbed comprising 1 normal and 24 fault classes under four attack scenarios demonstrate diagnostic accuracies of 96.6% (bias), 94.0% (noise), 92.8% (data replacement), and 95.7% (replay), while sustaining 96.7% under attack-free conditions. These results establish FO-MADS as a cost-effective and readily deployable solution that markedly enhances the cyber-physical resilience of IBR-dominated microgrids.

***Index Terms*—Fractional-order derivatives, single-point measurement, cyber-resilient fault diagnosis, inverter-based resource-dominated microgrids, hierarchical diagnosis, adversarial training.**

I. Introduction

Modern power systems are experiencing rapid growth in distributed energy resources (DERs) such as solar photovoltaics, wind turbines, and battery storage [1]. Inverter-based resource-dominated microgrids (IBR-dominated microgrids) integrate these DERs and, through power electronic converters (inverters), interface renewable generation and storage with the grid [1], [2]. Converter failures can jeopardize IBR-dominated microgrid stability, so continuous monitoring and robust diagnostics are required [1], [2]. Recent studies have proposed data-driven monitoring techniques [3], [4], yet open-circuit faults in insulated-gate bipolar transistor (IGBT) switches can still evade detection and cause phase current imbalance, torque ripple, and power quality degradation [5].

Conventional converter fault diagnosis is typically model-based or signal-based [6]. Model-based schemes rely on accurate system parameters and are sensitive to drift, whereas signal-based methods can be fragile to noise and changes in operating conditions [6], [7]. At the same time, integrating information and communication technology (ICT) exposes IBR-dominated microgrids to cyber vulnerabilities such as false data injection (FDI), denial-of-service (DoS), and deception attacks [8], [9]. These cyber threats complicate diagnosis and have motivated attack-resilient control strategies [6], [9], [10].

With the rapid development of artificial intelligence, data-driven fault diagnosis for power converters has become a major trend [11]–[14]. Machine learning models map sensor data directly to fault categories, enabling rapid detection without explicit physical models [11], [12]. However, their performance may degrade with low-quality data or unseen operating scenarios, especially when they depend on *multi-point* measurements that increase cost and complexity [4], [12]. Moreover, most existing studies still assume attack-free conditions and do not explicitly address concurrent cyber-attacks during fault diagnosis [6], [8], [15]–[19].

To fill these research gaps, this paper proposes FO-MADS, a unified framework that is both measurement-efficient and cyber-resilient. FO-MADS detects and localizes inverter open-circuit faults using only a single measurement point (volt-

979-8-3315-8138-1

age and power at the point of common coupling (PCC)) while simultaneously monitoring for cyber-attacks. Fractional-order signal processing constructs a dual-feature library: the Caputo derivative accentuates high-frequency perturbations for fault detection, whereas the Grünwald-Letnikov derivative emphasizes slow drifts for stealthy cyber-attacks. A two-stage hierarchical classifier localizes the faulty inverter (Stage 1) and pinpoints the specific faulty IGBT switch (Stage 2) [12], [13], while adversarial training is integrated via PMR-AT to improve robustness under diverse attack scenarios [20]–[22].

The main contributions are: (i) *Single-point, dual-fractional feature fault diagnosis*: A framework requiring only one PCC measurement with complementary fractional-order derivatives. (ii) *Hierarchical fault localization*: Two-stage strategy isolating faulty inverter and pinpointing faulty IGBT switch. (iii) *Cyber-resilient fault diagnosis*: PMR-AT ensures robust performance under cyber-physical disturbances.

The proposed FO-MADS bridges signal processing, machine learning, and cyber-security, providing a cost-effective route to improve IBR-dominated microgrid reliability. Effectiveness is validated on a multi-inverter testbed under various faults and cyber-attacks. The overall architecture of the proposed FO-MADS framework is depicted in Fig. 1.

II. Proposed FO-MADS Framework

FO-MADS utilizes single-point PCC data (V, P, Q) to classify 25 operational states across four inverters [20]–[22]. As illustrated in Fig. 1, the framework consists of dual-definition fractional-order feature extraction, a hierarchical diagnostic architecture, and adversarially robust training.

A. Dual-Definition Fractional-Order Feature Engineering

Two fractional operators capture complementary dynamics [23]: 1) **Caputo Derivative** (micro-perturbation detection):

$$ {}^{C}D_t^{\alpha} f(t) = \frac{1}{\Gamma(1-\alpha)} \int_0^t (t-\tau)^{-\alpha} f'(\tau)\, d\tau. \tag{1}$$

As shown in Fig. 2, the Caputo derivative enhances high-frequency transients in the VPQ signals, making subtle switching faults more separable in the feature space.

2) **Grünwald-Letnikov Derivative** (slow-drift detection):

$$ {}^{GL}D_t^{\beta} f(t) = \lim_{h\to 0} h^{-\beta} \sum_{k=0}^{\lfloor t/h \rfloor} (-1)^k \binom{\beta}{k} f(t-kh). \tag{2}$$

Similarly, Fig. 3 illustrates that the Grünwald-Letnikov derivative is more sensitive to slow-drift anomalies that are characteristic of stealthy cyber-attacks and data manipulation.

The combined feature vector:

$$ \mathbf{F}(t) = \left[{}^{C}D_t^{\alpha}V, {}^{C}D_t^{\alpha}P, {}^{C}D_t^{\alpha}Q, {}^{GL}D_t^{\beta}V, {}^{GL}D_t^{\beta}P, {}^{GL}D_t^{\beta}Q \right]^T . \tag{3}$$

Parameters: $\alpha = 0.7$, $\beta = 0.3$, $L = 400$ samples. The impact of these hyper-parameters on validation accuracy is further analyzed in Fig. 4.

B. Hierarchical Diagnostic Architecture

Two-stage classification addresses class imbalance: 1) Stage 1: 5-class inverter localization (normal + 4 inverters) and 2) Stage 2: 6-class switch isolation (activated only if a fault is detected). This hierarchical strategy significantly improves switch-level accuracy compared to flat classifiers. The sensitivity of the classifier to the Caputo order α and window length L is summarized in Fig. 4, which guides the empirical selection of working points.

C. Robustness Training

Progressive Memory-Replay Adversarial Training (PMR-AT) employs a curriculum of progressively stronger attacks, as sketched in Fig. 5: PGD-based adversarial example generation, Online Hard Example Mining (OHEM), historical attack replay, and progressive attack escalation. The adaptive attack-aware loss weighting schedule used to balance clean and adversarial samples during ablations is shown in Fig. 6.

Training curriculum: normal $\rightarrow$ bias $\rightarrow$ noise $\rightarrow$ replacement $\rightarrow$ replay.

III. Progressive Memory-Replay Adversarial Training

PMR-AT enhances robustness through 1) multi-stage attack escalation, 2) PGD attacks with $\epsilon = 0.1$, 3) historical attack replay, and 4) difficulty progression. The overall pipeline of PMR-AT, including the memory replay buffer and the curriculum of attack stages, is illustrated in Fig. 5, while Fig. 6 depicts the evolution of the attack-aware weight used in the loss function.

Attack-aware loss function:

$$ L_{\text{total}} = L_{\text{CE}}(y, \hat{y}) + \lambda \cdot \mathbb{E}_{(x_h, y_h)\sim\mathcal{D}_{\text{hard}}}[L_{\text{CE}}(y_h, f(x_h))], \tag{4}$$

where OHEM selects top-20% hard samples, with adaptive weight λ scaling with attack difficulty. The weight λ is defined as $\lambda = 0.5 \cdot d$, where $d \in [0, 1]$ represents the normalized attack difficulty (bias: 0.2, noise: 0.4, replacement: 0.7, replay: 1.0).

IV. Simulation and Experimental Results

A. Experimental Setup

A Simulink-based four-inverter testbed generated 5,600 VPQ samples (50 Hz, 2 kHz sampling) with: 24 fault classes (single IGBT open-circuit), 4 attack types (bias, noise, replacement, replay), and an 80/20 train-test split. Bias attacks inject a 10% DC offset in VPQ, while Gaussian noise attacks use $\sigma = 5\%$ of the nominal magnitude; replacement attacks randomly substitute 20% of samples with stale measurements. The detailed configuration of the IBR-dominated microgrid and the single VPQ measurement point used for diagnosis are shown in Fig. 7.

979-8-3315-8138-1

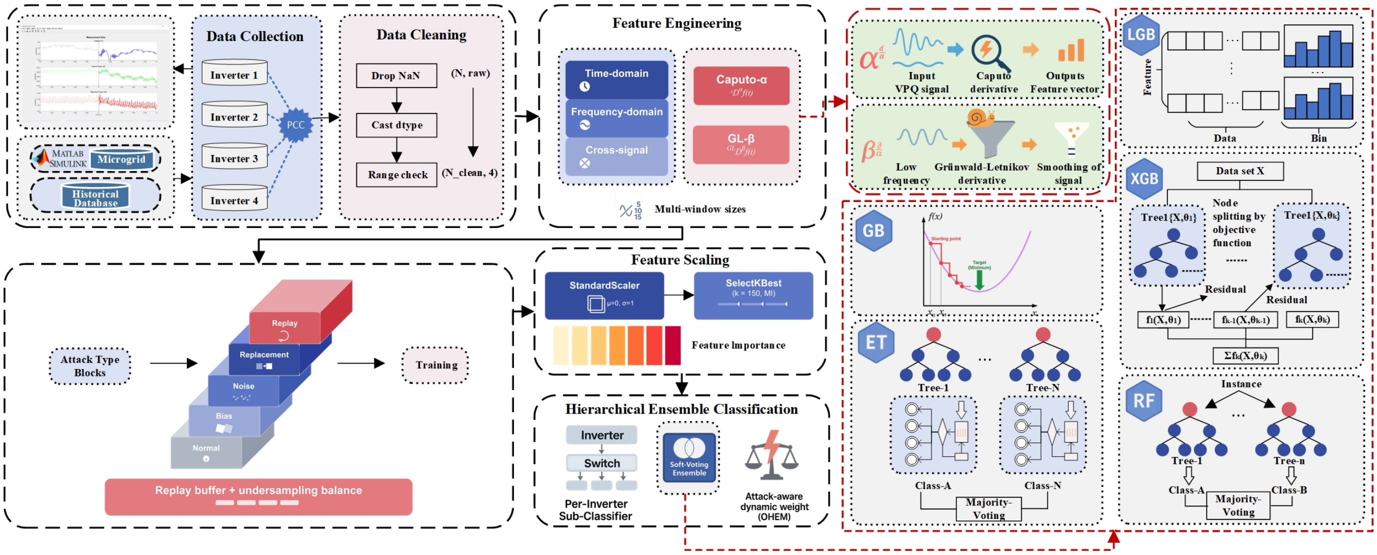

Fig. 1. Main framework of the FO-MADS

TABLE I
OVERALL CLASSIFICATION ACCURACY (%)

Method	Normal	Bias	Noise	Replacement	Replay	Remarks
FO-MADS (Proposed)	96.7	96.6	94.0	92.8	95.7	Full implementation with all components
FO-MADS w/o OHEM	95.1	94.3	90.2	87.5	92.0	Without Online Hard Example Mining
FO-MADS w/o Frac. Feat.	93.8	92.6	88.1	85.3	90.4	Without fractional-order features
XGBoost	93.7	93.3	88.9	83.9	91.2	Baseline model 1
Random Forest	93.5	93.1	88.2	83.2	91.5	Baseline model 2
CNN	92.0	90.5	85.8	80.1	88.9	Baseline model 3

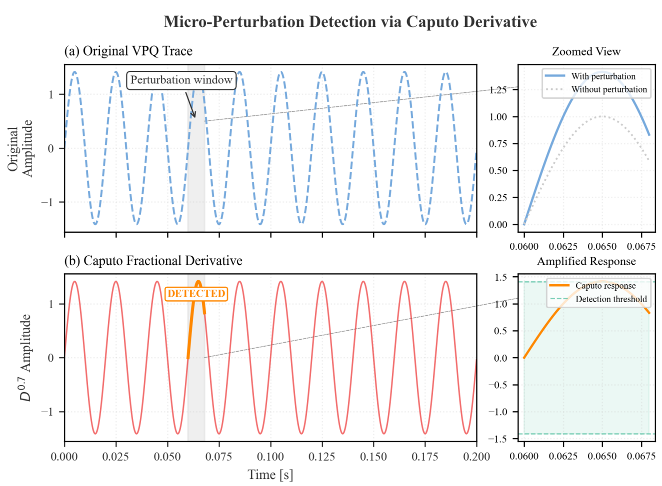

Fig. 2. Process of Caputo derivative on VPQ signals showing enhanced detection of high-frequency transients

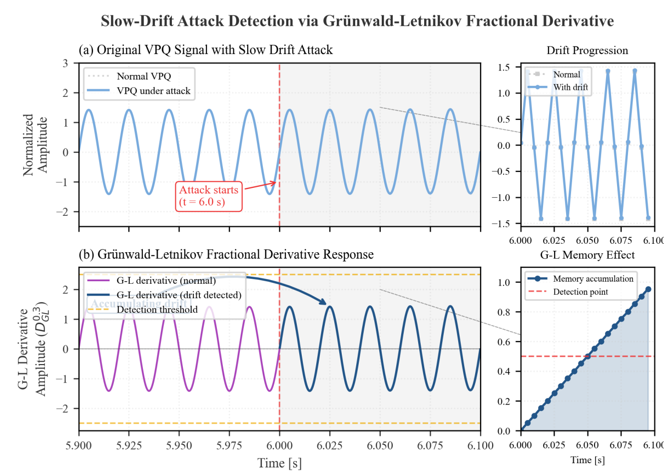

Fig. 3. Process of Grünwald-Letnikov derivative on VPQ signals showing enhanced detection of slow-drift anomalies

B. Performance Evaluation

FO-MADS achieves high accuracy across all scenarios, as summarized in Table I. A visual comparison of FO-MADS with several baseline models under different attack types is provided in Fig. 8, while Fig. 9 presents a heat-map view of model performance across attack scenarios.

Hierarchical breakdown is reported in Tables II and III. Specifically, inverter localization remains above 94.8% under all attack types, as shown in Table II, while switch isolation maintains above 95.8% accuracy even in adversarial cases, as summarized in Table III.

979-8-3315-8138-1

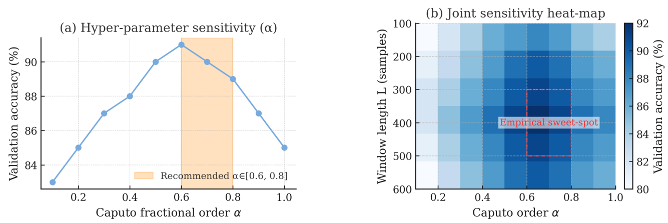

Fig. 4. Hyper-parameter study of FO-MADS. (a) Validation accuracy versus Caputo fractional order α ($\beta = 0.3$, $L = 400$). (b) Joint sensitivity heat-map of α and window length L; darker color denotes higher accuracy. The red rectangle marks the empirical sweet-spot

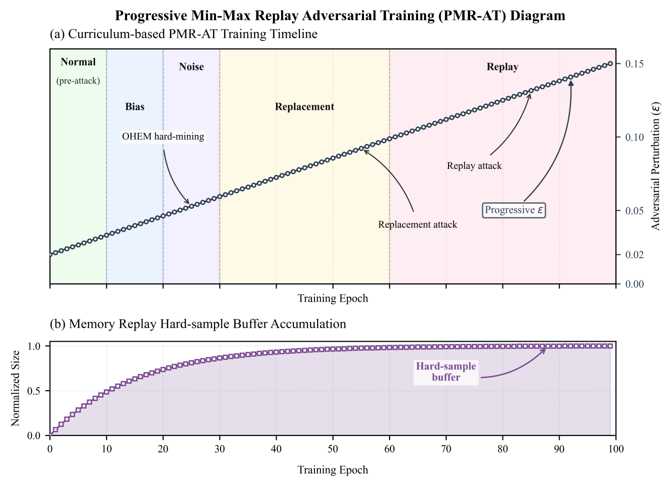

Fig. 5. Illustration of the PMR-AT training procedure showing progressive attack escalation and memory replay mechanism

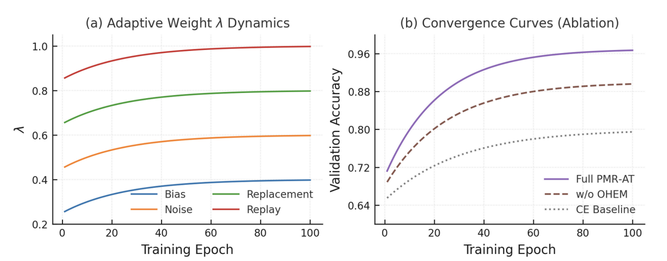

Fig. 6. Adaptive weight dynamics across components and convergence curves from ablation experiments

TABLE II
INVERTER-LEVEL ACCURACY (%)

Attack Type	Normal	Bias	Noise	Replacement	Replay
FO-MADS	97.4	98.5	96.0	94.8	96.3

TABLE III
SWITCH-LEVEL ACCURACY (%)

Attack Type	Normal	Bias	Noise	Replacement	Replay
FO-MADS	99.2	97.6	97.0	95.8	99.3

Ablation analysis confirms the benefit of the proposed components (see Fig. 10): dual fractional features boost noise and replacement robustness by 5.9% and 7.5%, respectively; OHEM further reduces switch-level misclassification under noise; and PMR-AT enhances replay-attack resilience. The corresponding attack-wise model comparison and scenario-wise performance, including additional baselines (LightGBM, SVM, and ELM) beyond those summarized in Table I, are depicted in Fig. 8 and Fig. 9.

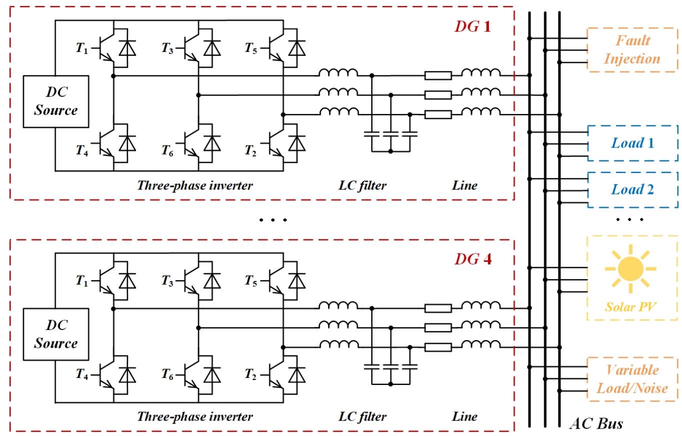

Fig. 7. Simulink-based four-inverter IBR-dominated microgrid testbed for experimental validation

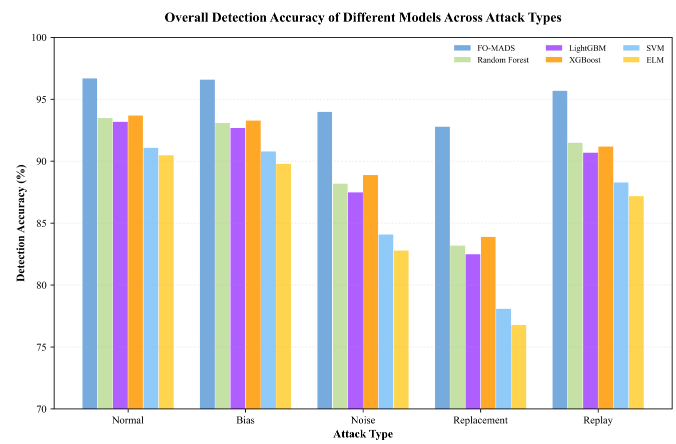

Fig. 8. Overall detection accuracy of different models across attack types

V. Conclusions

This study introduced FO-MADS, a cost-effective framework achieving cyber-physical resilience for inverter-based resource-dominated microgrids using only a single VPQ sensor. By exploiting Caputo and Grünwald-Letnikov derivatives, FO-MADS constructs a dual fractional-order feature library that magnifies both high-frequency perturbations and slow-drift anomalies. A two-stage hierarchical classifier localizes the faulty inverter and isolates the defective IGBT switch, while PMR-AT systematically hardens the model against cyber-attacks. Extensive simulations yielded 96.7% accuracy under attack-free operation and above 92.8% across all attack scenarios.

979-8-3315-8138-1

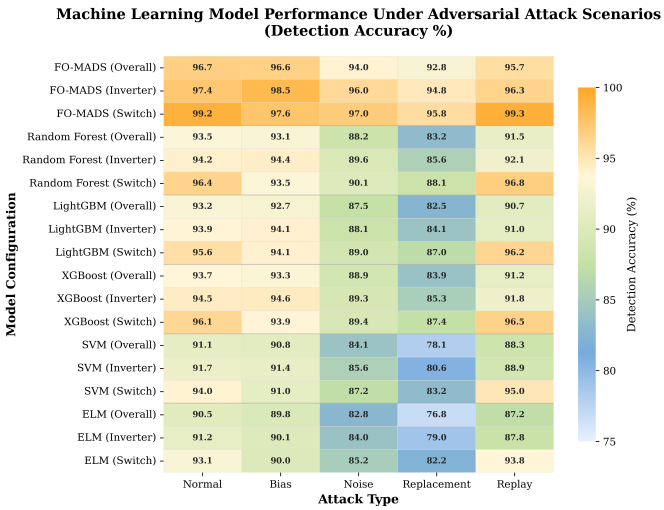

Fig. 9. Machine learning model performance under adversarial attack scenarios

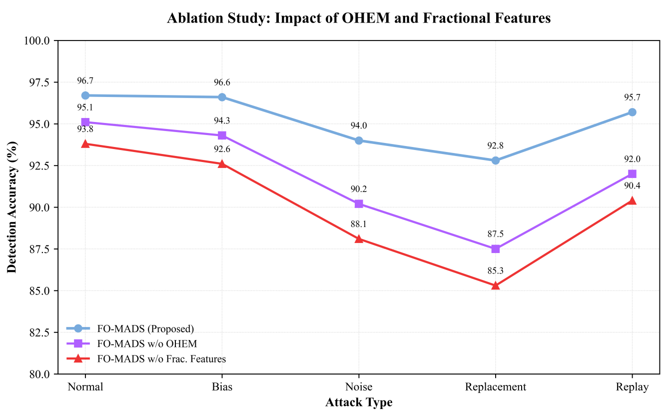

Fig. 10. Ablation study impact of OHEM and fractional features

The main contributions include: 1) single-sensor diagnosis eliminating multi-point instrumentation; 2) dual-definition feature engineering using complementary fractional operators; 3) hierarchical localization significantly improving switch-level accuracy; and 4) cyber-resilient fault diagnosis with PMR-AT that significantly improves adversarial accuracy across diverse attack types.

Future work will focus on hardware-in-the-loop trials, embedded implementations, extended fractional-order features, and distributed privacy-preserving variants, advancing FO-MADS toward fully deployable real-time solutions for resilient power distribution networks.

References

[1] A. Hirsch, Y. Parag, and J. M. Guerrero, “Microgrids: A review of technologies, key drivers, and outstanding issues,” *Renew. Sustain. Energy Rev.*, vol. 90, pp. 402–411, Mar. 2018.

[2] S. Yang, D. Xiang, A. Bryant, P. Mawby, L. Ran, and P. Tavner, “Condition monitoring for device reliability in power electronic converters: A review,” *IEEE Trans. Power Electron.*, vol. 25, no. 11, pp. 2734–2752, Nov. 2010.

[3] Y. Hu, Y. Song, X. He, X. Zhao, X. Yang, J. Yao, Z. Wang, H. Pei, and C. Hu, “MAACCN: An intelligent decoupling diagnosis method for compound faults in electro-hydrostatic actuators,” *IEEE Trans. Instrum. Meas.*, vol. 74, pp. 1–11, 2025.

[4] L. Kong, Y. Mao, T. Zhang, X. Chen, Z. Wang, and X. Wang, “Online data-driven diagnosis for common electrical and sensor faults in dual three-phase PMSM drives,” *IEEE Trans. Instrum. Meas.*, vol. 74, pp. 1–10, 2025.

[5] X. Ge, J. Pu, B. Gou, and Y.-C. Liu, “An open-circuit fault diagnosis approach for single-phase three-level neutral-point-clamped converters,” *IEEE Trans. Power Electron.*, vol. 33, no. 3, pp. 2559–2567, Mar. 2018.

[6] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, A. Abusorrah, L. Che, and X. Liu, “Cross-Layer Distributed Control Strategy for Cyber Resilient Microgrids,” *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 3705–3717, Sep. 2021.

[7] W. Yao, Y. Wang, Y. Xu, and C. Deng, “Cyber-resilient control of an islanded microgrid under latency attacks and random DoS attacks,” *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 5858–5869, Apr. 2023.

[8] D. Shi, P. Lin, Y. Wang, C.-C. Chu, Y. Xu, and P. Wang, “Deception attack detection of isolated DC microgrids under consensus-based distributed voltage control architecture,” *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 11, no. 1, pp. 155–165, Mar. 2021.

[9] H. Shen, Y.-A. Liu, K. Shi, J. H. Park, and J. Wang, “Event-based distributed secondary control for AC islanded microgrid with semi-Markov switched topology under cyber-attacks,” *IEEE Syst. J.*, vol. 17, no. 2, pp. 2927–2939, Jun. 2023.

[10] Y. Xia, Y. Xu, Z. Wang, and F. Li, “A data-driven method for online gain scheduling of distributed secondary controller in time-delayed microgrids,” *IEEE Trans. Power Syst.*, vol. 39, no. 3, pp. 5036–5046, May 2024.

[11] Y. Xia and Y. Xu, “A robust data-driven method for open-circuit fault diagnosis of power switches in three-phase inverters with low-quality data,” *IEEE Trans. Power Electron.*, vol. 40, no. 4, pp. 5949–5958, Apr. 2025.

[12] Y. Xia, Y. Xu, and N. Zhou, “A transferrable and noise-tolerant data-driven method for open-circuit fault diagnosis of multiple inverters in a microgrid,” *IEEE Trans. Ind. Electron.*, vol. 71, no. 7, pp. 8017–8028, Jul. 2024.

[13] Y. Xia and Y. Xu, “A transferrable data-driven method for IGBT open-circuit fault diagnosis in three-phase inverters,” *IEEE Trans. Power Electron.*, vol. 36, no. 12, pp. 13478–13485, Dec. 2021.

[14] 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. 3690–3698, Sep. 2020.

[15] Q. Deng et al., “A high-accuracy light-AI data-driven diagnosis method for open-circuit faults in single-phase PWM rectifiers,” *IEEE Trans. Transp. Electrific.*, Early Access, 2023.

[16] Z. Huang and Z. Wang, “A multiswitch open-circuit fault diagnosis of microgrid inverter based on slidable triangularization processing,” *IEEE Trans. Power Electron.*, vol. 36, no. 1, pp. 922–930, Jan. 2021.

[17] B. Gou, Y. Xu, Y. Xia, G. Wilson, and S. Liu, “An intelligent time-adaptive data-driven method for sensor fault diagnosis in induction motor drive system,” *IEEE Trans. Ind. Electron.*, vol. 66, no. 12, pp. 9817–9827, Dec. 2019.

[18] B. Gou, Y. Xu, Y. Xia, and Q. Deng, “An online data-driven method for simultaneous diagnosis of IGBT and current sensor fault of three-phase PWM inverter in induction motor drives,” *IEEE Trans. Power Electron.*, vol. 35, no. 12, pp. 13281–13289, Dec. 2020.

[19] M. A. M. Radzi, A. H. A. Baker, M. K. M. Jamil, and H. H. Goh, “Microgrid fault detection and classification: Machine learning based approach, comparison, and reviews,” *Energies*, vol. 13, no. 13, p. 3460, 2020.

[20] M. R. Shadi, M. T. Ameli, and S. Azad, “A real-time hierarchical framework for fault detection, classification, and location in power systems using PMU data and deep learning,” *Int. J. Electr. Power Energy Syst.*, vol. 134, Art. no. 107399, 2022.

[21] X. Liu and Z. Li, “Masking transmission line outages via false data injection attacks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 7, pp. 1592–1602, Jul. 2016.

[22] S. Saha, T. K. Roy, M. A. Mahmud, M. E. Haque, and S. N. Islam, “Sensor fault and cyber-attack resilient operation of DC microgrids,” *Int. J. Electr. Power Energy Syst.*, vol. 99, pp. 540–554, 2018.

[23] B. T. Krishna, “Studies on fractional order differentiators and integrators: A survey,” *Signal Process.*, vol. 91, no. 3, pp. 386–426, Mar. 2011.