Enhanced Real-Time ATM-Based MPC for Electric Vehicles With Cyber–Physical Security Aspect

Ali Arsalan, *Graduate Student Member, IEEE*, Behnaz Papari, *Senior Member, IEEE*, Laxman Timilsina, *Member, IEEE*, Grace Muriithi, *Graduate Student Member, IEEE*, Ali Moghassemi, *Graduate Student Member, IEEE*, S. M. Imrat Rahman, *Graduate Student Member, IEEE*, Elutunji Buraimoh, *Graduate Student Member, IEEE*, Gokhan Ozkan, *Senior Member, IEEE*, and Christopher S. Edrington, *Senior Member, IEEE*

***Abstract*— Inverter-based electric drive systems (EDSs) in electric vehicles (EVs) are susceptible to various common cyber and physical anomalies (CPAs), such as cyberattacks (CAs) and open-circuit faults (OCFs) in power switches. Most existing data-driven diagnostic schemes for motor drives solely rely on residual and three-phase output current signals and are prone to misclassification due to overlapping data features associated with these anomalies. Moreover, these methods concentrate on detecting either CAs or OCFs independently, lacking a unified approach that can be universally applied to both types of anomalies. Therefore, in this work, a physics-informed machine learning (PIML) approach is proposed, which can effectively distinguish between CAs and OCFs in EDS. In this regard, the unique features associated with stator current, resulting from various CPAs, are used to estimate the stator voltage characteristics through a synchronous motor mathematical model. The proposed voltage-based features characterizing better correlation via distinctive EDS transients in response to these anomalies are further used as the system's prior information by a machine learning (ML) classifier. Moreover, active thermal management (ATM)-based model predictive control (MPC) is utilized in the control layer due to its benefits in device-level thermal cycling and power quality. In addition, various variations in electrical, mechanical, and thermal characteristics due to CPAs in EDS have also been analyzed. The presented approach is evaluated for the US06 standard drive cycle in real time via controller-hardware-in-the-loop (CHIL) experiment for various case study scenarios, resulting in a classification accuracy of 98.92%.**

***Index Terms*— Active thermal management (ATM)-based model predictive control (MPC), cyberattacks (CAs), electric drive system (EDS), physical fault detection, physics-informed machine learning (PIML).**

NOMENCLATURE

Abbreviations

PIML	Physics-informed machine learning.
CHIL	Controller hardware in the loop.
FFT	Fast Fourier transform.
CNN	Convolutional neural network.
LSTM	Long short-term memory.
DoS	Denial of service.
SS	Single switch.
SDS	Series-double switch.
CDS	Cross-double switch.
PDS	Parallel-double switch.
CAN	Controller area network.
FDI	False data injection.
FOC	Field-oriented control.
NPC	Neutral point clamped.
PEC	Power electronics.
VCRP	Voltage current and reactive power.
IPMSM	Interior permanent magnet synchronous motor.
IVCN	In-vehicle communication network.
RNN	Recurrent neural network.
FNN	Feedforward neural network.
EMT	Electrical mechanical and thermal.
CA	Cyberattack.
LIN	Local interconnect network.
UDP	User datagram protocol.
MTPA	Maximum torque per ampere.
OCF	Open-circuit fault.
CPA	Cyber and physical anomaly.
EV	Electric vehicle.
ECU	Electronic control unit.
EDS	Electric drive system.
ATM	Active thermal management.
MPC	Model predictive control.

Notations

I_{abc}	Three-phase Stator current.
$T_{\text{ipmsm}}^{\text{ref}}$	Electromagnetic IPMSM reference rotor torque.
ω_m^{fb}	IPMSM feedback rotor speed.
ω_m^{ref}	IPMSM reference rotor speed.
X_r^{ref}	Residual values.
k	Sampling instant.
V_{dc}	DC bus voltage.
T_j	MOSFET's junction temperature.
P, R, $F1$	Precision, recall, and F1-score.
Acc	Classification accuracy.
$S_{1,2,\ldots,6}$	Power switches 1–6.
ω_s	Window size.

Received 28 May 2024; revised 14 August 2024; accepted 23 September 2024. Date of publication 26 September 2024; date of current version 3 February 2025. This work was supported by the U.S. Army DEVCOM Ground Vehicle Systems Center (GVSC) through the Simulation-Based Reliability and Safety Program for Modeling and Simulation of Military Ground Vehicle Systems under Grant W56HZV-17-C-0095. *(Corresponding author: Ali Arsalan.)*

The authors are with the Secure Energy and Automation Laboratory (SEAL) and the Real-Time COntrol and Optimization Laboratory (RT-COOL), Clemson University, Clemson, SC 29634 USA (e-mail: aarsala@clemson.edu; bpapari@clemson.edu; ltimils@clemson.edu; gmuriit@clemson.edu; amoghas@clemson.edu; smimrar@clemson.edu; eburaim@clemson.edu; gokhano@clemson.edu; cedring@clemson.edu).

Digital Object Identifier 10.1109/TTE.2024.3468887

Δt	Learning rate.
T_{det}	Detection time.
T_{ws}^{d}	Window-size delay.
T_{compu}^{d}	Computational delay.
T_{com}^{d}	Communication delay.
θ_e	IPMSM rotor position angle.
$\text{Tgr}_{(\text{sf})}$	Current sensor fault trigger.
$E_s(t)$	Current sensor energy consumption.
E_{rated}	Current sensor rated energy consumption.
$E_{\min}$	Minimum energy threshold.
$G_{1,2,\ldots,6}$	Gate drive signals for S_1–S_6.
$\vec{A}$	CAs' intensity vector.
$\vec{x}(t)$	EDS's compromised signals instantaneous values.
$\vec{t}_{\text{ca}}$	Time duration of CAs.
I_{dq}	dq-axis feedback IPMSM current.
v_{dq}	dq-axis feedback IPMSM voltage.
I_{dq}^{ref}	dq-axis reference current.
T_e	Electromagnetic IPMSM rotor torque.

I. Introduction

In recent years, the automotive sector has seen an unprecedented digital transformation toward a closely connected Internet of Things (IoT)-based infrastructure. Therefore, automobiles have evolved from conventional confined systems to software-defined vehicles with better connectivity, coordination, and flexibility. However, these IoT-based modern mobility applications also highlight the security and privacy concerns, subject to vulnerabilities of CAN bus toward CAs for various safety-critical EV systems. According to the Global Automotive Cybersecurity Report 2023, 14% of CAs were instigated on ECUs and 35% of CAs were instigated on telematics and application servers in 2022 [1]. In addition, the vast communication network linked with ECUs also increases the attack surface for invaders. A compromised EDS, resulting from a data-integrity attack, can give rise to fluctuations in feedback and reference signals in cyber layer [2] while severely impacting the traction control stability and endangering the occupant's safety. In this regard, the cyber–physical security of modern EV PEC systems, in the context of impact analysis and EV's vulnerability under various CAs, has been presented in [3] and [4].

Furthermore, apart from EDS vulnerability to CAs, Julian and Oriti [5] and Klug and Griggs [6] highlight the reliability of multiple subsequent components of EDS in terms of failure rate. These findings indicate that the Hall effect current sensor has the highest reliability, ranging from 400 to 2000 FIT (1 FIT = 1 failure within 10^9 h), while the power converter is the least reliable component in EDS, with its reliability ranging from 1000 to 70 000 FIT. Therefore, power converters are considered in this study from a physical fault perspective. Notably, within the power converter, the power switches are the most susceptible element, particularly prone to the common OCFs that account for up to 38% of total inverter faults [7]. These faults pose significant challenges to a sustained system operation by causing extreme mechanical vibrations, electromagnetic torque distortions, and current fluctuations. Hence, various substantial methods, classified as model-based and data-driven strategies, for detecting OCFs and CAs are presented in the literature to ensure a reliable, safe, and continuous operation of EDS.

The model-based methods require an explicit system model, where the predicted values are obtained via a linear dynamic system-based state estimation model and compared with measured outputs to reflect the presence of a CA [8], [9], [10]. In this context, a state observer-based approach is presented in [11] to detect cyber–physical attacks in EV's lateral stability control system and motor drive. In addition, a novel index-based matrix approach for performance degradation quantification of the motor drive is presented, which is further used for CA detection [4], [11]. Similarly, model-based schemes are also extensively being used for OCF diagnosis, using observer-based methods [12], parity equations [13], and state estimation schemes [14] to formulate an explicit mathematical model of the system, which can be further used to estimate system's state values. The model-based schemes offer a relatively fast diagnosis without any additional hardware. However, these methods are not preferred due to the high dependence on the accuracy of the system model, which can lead to problems associated with modeling complexity and parameter uncertainties in the working environment.

On the other hand, data-driven approaches can be applied to time-varying and complex nonlinear systems without relying on the system's model, pre-tuned thresholds, and load patterns. The limitation of data scarcity associated with this approach can be addressed by collecting the system's data in different operating conditions using reliable real-time simulators such as OPAL-RT, Typhoon, and Speedgoat. Moreover, transfer-learned models can also be adapted for limited experimental data while achieving satisfactory accuracy [15]. Furthermore, compared to the sturdy algorithms of model-based methods, data-driven schemes exhibit superior generalization performance, making this approach suitable for diagnosing various adjacent CPAs in EDS.

In the context of data-driven schemes, an FFT-based method is applied to EDS's data for detection and classification between CAs and traction motor-based physical faults in [16]. Moreover, apart from using frequency-domain features, various time-domain statistical features as diagnostic signals can also be used with a data-driven classifier [17], [18]. In this regard, a fast detection approach for an EV is demonstrated in [19], where data features, such as mean, variance, kurtosis, and skewness, are extracted from trustworthy time-series sensor signals of EDS, which are then fed into four different binary classifiers for CA detection. In [15], a transfer learning-based scheme is presented, where a CNN is initially trained by utilizing extensive simulation data of a motor drive system. After that, the network is fine-tuned with minimal experimental data by using transfer learning, resulting in outstanding performance for CA detection. Furthermore, Arsalan et al. [18] and Guo et al. [20] introduce a PIML approach to distinguish between normal operation and a CA in EDS. The PIML approach demonstrates superior performance compared to purely data-driven and model-based methods [21]. Similarly, in [22] and [23], CNN-based fault diagnosis methods are

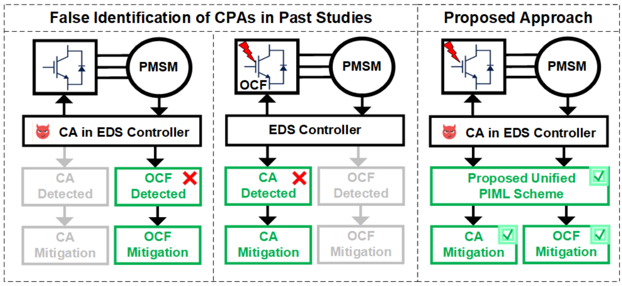


Fig. 1. Limitations in past studies and the proposed solution.

proposed, where time-domain diagnostic signals are converted into 2-D images for OCF feature extraction. Moreover, various signal preprocessing techniques, such as FFT, principle component analysis, wavelet packet transform, and FFT+Relief, are used for input data dimensionality reduction and highly correlated feature extraction in [24], [25], [26], [27], [28], and [29]. These methodologies further utilize random vector functional link, Bayesian networks, multiclass relevance vector machine, LSTM, and extreme learning machine-based RVFL for OCF diagnosis in power converters.

A. Contributions

To the best of our knowledge, in all of the previously published research, the CAs and OCFs diagnosis algorithms are proposed independently. In addition, it is important to note that the input data features used by classifiers for detecting OCFs and CAs can often be quite similar, particularly in residual-based diagnostic schemes such as those discussed in [11], [20], [36], and [37]. However, for effective multiclass classification, heterogeneity in the input dataset is a key characteristic that must be considered. In addition, for methods that primarily analyze current signals for OCF diagnosis [24], [38], [39], DoS-based CAs can readily mimic the behavior of SDS-OCF, leading to potential misdiagnosis of these atypical events. Thus, current schemes are vulnerable due to their inability to distinguish between OCFs and CAs within an EDS. This, in return, can mislead the controller into implementing incorrect mitigation responses, as illustrated in Fig. 1. To address this issue, we propose a unified PIML-based online diagnosis scheme that is designed to simultaneously detect and accurately distinguish between OCFs related to power switches and common CAs in EDS. Furthermore, to emphasize the contributions of this article, Table I presents a comparative analysis of several previous studies, including their limitations and practical implications. Moreover, the contributions of this study can also be summarized as follows.

1) A new feature extraction dataset, based on the magnitude of stator voltages in the dq-axis of the EDS, is introduced. This dataset offers distinct characteristics associated with the OCFs and CAs being tested, thereby providing valuable prior information to a machine learning (ML) classifier for the detection and classification of CPAs. As a result, it enhances the ability to accurately respond and mitigate the effects of CAs or OCFs.
2) This study investigates the impact of various single and double-switch OCFs in the power converter, along with CAs such as FDI and DoS attacks targeting the feedback and reference signals of the EDS controller, on the electrical, mechanical, and thermal characteristics of the EDS. Notably, the analysis of thermal characteristics, in particular, represents a novel aspect that has not been previously explored in the existing literature.
3) The offline classification accuracy of the proposed unified approach for various CPAs is compared with a conventional residual-based scheme via different ML classifiers. The suggested approach provides higher efficiency and generalization performance in detecting CAs and OCF-based physical faults.
4) To substantiate the practical applicability, the proposed PIML approach is not only validated offline using an LSTM-based multiclass classifier but also assessed in real time through a CHIL experimental setup using the US06 drive cycle, resulting in an accuracy of 98.92%.

In this article, Section II illustrates the ATM-based MPC for EDS. Section III comprises disturbance characterization in terms of CAs modeling. Section IV describes the physics-based EDS features and ML algorithm's architecture. Section V consists of the real-time simulation results on impact analysis and CPAs detection via CHIL experiment. Finally, Section VI consists of the conclusion.

II. ATM-Based MPC Design for Motor Drive

The structure of a modern EV generally consists of one or more motors connected with a battery pack, traction inverter, and various other control components. All system- and device-level control signals are transmitted via CAN buses, FlexRay communication, and LIN. Moreover, works [2], [4], [11], [16], [19], [20], [24] focus on either FOC or traditional MPC for the control framework. However, the ATM-based MPC, a promising approach for motor drives due to its thermal aspects, has yet to be explored. In this regard, MPC is configured with ATM by coupling power converters' electrical and thermal attributes in an objective function, showcasing an ATM-based MPC control [40]. This ATM-based MPC approach reduces MOSFETs' life degradation and fault occurrence rate by considering their junction temperature to obtain optimal switching states. The traction inverter's predicted current and temperature values for ATM-based MPC control are illustrated in [41] and [42]. A simplified RC network known as a lumped parameter thermal network is used to model the thermal states of semiconductor devices analytically [40]. The characteristics obtained from the datasheet of the SiC half-bridge module-Cree/Wolfspeed CAB530M12BM3 (1200 V and 530 A) are used for the power loss modeling. The detailed schematic of the ATM-based MPC model for an EDS is shown in Fig. 2.

III. Disturbance Characterization in Cyber and Physical Layers

This study interprets disturbances as disruptions originating from CAs and OCFs. In this regard, the associated labels of each CPA considered in this study are shown in Table II.

TABLE I

CHARACTERISTICS AND LIMITATIONS OF PAST STUDIES AND THE PROPOSED APPROACH

Methods (Year)	Investigated system	Power converter switching control	Anomalies modes	Impact analysis and Diagnosis	Limitation/Real-world impact
[16] (2022)	Dual-motor EV powertrain	Field-oriented control	False data injection attacks, Inter-turn short circuit and motor bearing faults	Impact analysis on 3-phase current, Detection of cyber-attacks and common physical faults	*Physical faults in power switches caused by OCFs are not differentiated from cyber-attacks. *Existing anomaly detection schemes, when implemented independently, often lead to higher computational and implementation cost. So, adopting a unified approach could be more efficient and cost-effective. *OCFs and CAs can create a homogeneous impact on the system parameters, utilized by existing independent anomaly diagnosis algorithms. This similarity can lead to potential misdiagnosis. *Since the repair processes for major anomalies like CAs and OCFs differ significantly, inaccurate system state diagnosis can result in inappropriate mitigation response. This can lead to performance degradation, unnecessary shutdowns, and potential equipment damage.
[19] (2021)	EV traction motor drive	Field-oriented control	False data injection attacks	Impact analysis on 3-phase current, Cyber-attacks detection	
[20] (2020)	EV traction motor drive	Field-oriented control	False data injection and replay attacks	Impact analysis on stator current, Cyber-attacks detection	
[15] (2023)	Motor drive system	Field-oriented control	False data injection attacks	Impact analysis on stator current, Cyber-attacks detection	
[11] (2020)	EV traction motor drive	Field-oriented control	Data integrity, replay, and DoS attacks	Impact analysis on yaw rate, sideslip angle, lateral traveling distance and torque	
[4] (2019)	EV traction motor drive	Field-oriented control	Data integrity attacks	Impact analysis on speed, current and torque	
[30] (2022)	Grid-tied PV system	Current controller	Line-to-line (LL) fault, False data injection attacks replicating LL faults	Impact analysis on stator current, Cyber-attacks detection	
[31] (2021)	PEC-enabled PV farm	VCRP control loop-based controller	False data injection attacks	Impact analysis on stator voltage current and power, Cyber-attacks detection	
[32] (2022)	Active NPC PV converter	VCRP control loop-based controller	False data injection attacks	Impact analysis on 3-phase current, Cyber-attacks detection	
[33] (2023)	PEC-enabled PV farm	VCRP control loop-based controller	Data integrity and replay attacks, IGBT open-circuit, line-to-line and line-to-ground faults	Impact analysis on 3-phase voltage, current and power, Cyber-attacks detection	
[34] (2023)	PMSM motor drive system	Vector control	Single switch OCFs, Open phase faults	Impact analysis on 3-phase current, OCF and Open phase faults detected and distinguished	
[35] (2023)	PMSM motor drive system	Vector control	Single and double switch OCFs	Impact analysis on stator current, fault detection and localization	
[24] (2020)	Induction motor drive system	Vector control	Single and double switch OCFs, Current sensor faults	Impact analysis on 3-phase current, OCF and sensor fault detected and distinguished	
This work	**EV electric drive system**	**ATM-based MPC**	**False data injection, Denial of service, single and double switch OCFs**	***Impact analysis on stator current, stator voltage, speed, torque, and the junction temperature of power switches. *Detection and Differentiation between cyber-attacks and OCFs.**	

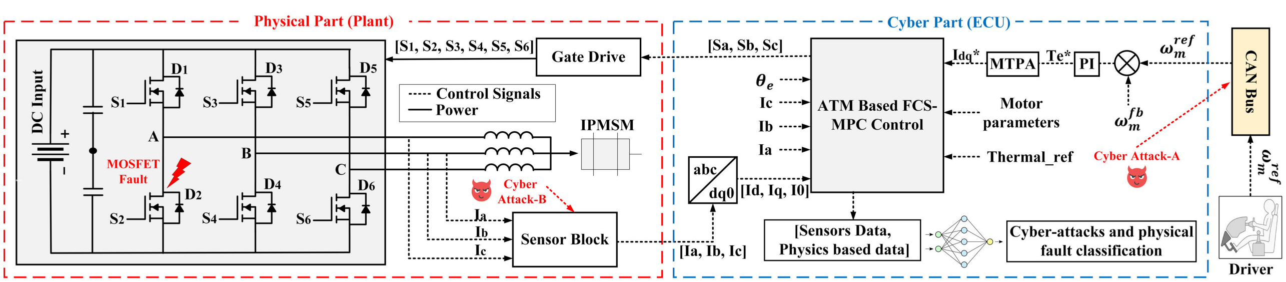


Fig. 2. Schematic of IPMSM motor drive with the vulnerable points toward CPAs.

A. CA Modeling

For vehicle cyber–physical security, the IVCN, ECU, and EDS are assumed to be vulnerable to external intrusions. Once the IVCN is hijacked, an attacker can easily superposition the false data with normal data on a high-speed EDS CAN bus (125 Kb/s–1 Mb/s). One of the most common CAs targeting EDS in most of the past studies is FDI and DoS attacks [2], [4], [11], [15], [16], [19], [20], [43]. Moreover, while evaluating the vulnerability of EDS to CAs, it is notable that the reference input and feedback signals are directly associated with the IVCN, making them more susceptible to anomalies [44]. Therefore, in this context, CAs are specifically conducted on I_a, I_b, I_c, ω_m^{ref}, and $T_{\text{ipmsm}}^{\text{ref}}$ for different case study scenarios. It is assumed that the attacker sniffed the arbitration IDs and byte numbers for these EDS's signals. Therefore, in each type of attack, the adversary can jeopardize the integrity of these standard operational signals by hijacking the CAN bus. Moreover, the signals affected by FDI and DoS attacks can be

TABLE II
DEFINITION AND LABELING OF CPAS IN EDS

Operational Modes	Categories of CPAs	Target Signals	No.s	Label
Open Circuit Faults in MOSFETs [24]	SS-OCF	(S1); (S2); (S3); (S4); (S5); (S6)	1-6	1
	SDS-OCF	(S1, S2); (S3, S4); (S5, S6)	7-9	
	CDS-OCF	(S1, S4); (S2, S3); (S3, S6); (S4, S5); (S1, S6); (S2, S5)	10-15	
	PDS-OCF	(S1, S3); (S2, S4); (S3, S5); (S4, S6); (S1, S5); (S2, S6)	16-21	
Cyber-attacks on EDS Signals	FDI [20] $\vec{A}$= {-0.75, -1.2, 1.2, 2, 5}	(Ia); (Ib); (Ic); (Ia, Ib); (Ib, Ic); (Ia, Ic); (Ia, Ib, Ic)	22-56	2
		(T_{ipmsm}^{ref}); (ω_m^{ref})	57-66	
	DoS: $\vec{A}$= {0}	(Ia); (Ib); (Ic); (Ia, Ib); (Ib, Ic); (Ia, Ic); (Ia, Ib, Ic)	67-73	
		(T_{ipmsm}^{ref}); (ω_m^{ref})	74-75	
Normal Operation				0

generically expressed as follows [20]:

$$\vec{X} = \begin{cases} \vec{A} \odot x(\vec{t}), & \text{for } t \in \vec{t_{\text{ca}}} \\ x(\vec{t}), & \text{otherwise} \end{cases} \tag{1}$$

where $\vec{X}$ indicates the vector of compromised EDS signals, tempered at different sampling instants and intensity values, formulated by using different values for different EDS signals, as listed in Table II.

B. OCF Modeling

Each phase of a two-level, three-phase inverter consists of two power transistors S_i and two antiparallel diodes D_i. The upper switch and lower diode can only conduct the positive current into machine winding, whereas the negative current can only flow through the upper diode and lower switch. Therefore, when there is an OCF in upper switch S_1, I_a will no longer have the positive current, and for OCF in S_2, I_a will have no negative current component [24]. Moreover, the OCFs for the single and double switches can be categorized as SS-OCF, SDS-OCF, CDS-OCF, and PDS-OCF, as depicted in Fig. 3. In addition, to model/simulate these OCF, the gating signal of the associated power switches is turned to zero [24] as follows:

$$G_{(S1-S6)} = [G_1, G_2, G_3, G_4, G_5, G_6]$$
$$y_{(G_{(S1-S6)})} = \begin{cases} [0, G_2, G_3, G_4, G_5, G_6], & \text{if SS-OCF} \\ [0, G_2, G_3, 0, G_5, G_6], & \text{if CDS-OCF} \\ G_{(S1-S6)}, & \text{otherwise} \end{cases} \tag{2}$$

where $G_{(S1–S6)}$ represents the gating signal for six power transistors during the normal operation. Moreover, $y_{(G_{(S1-S6)})}$ indicates the values of gating signals applied to power transistors. Therefore, based on (2), if there is an OCF in S_1 under the SS-OCF category, the gating signal applied to S_1 is turned to zero, whereas during the CDS-OCF scenario, the gating signal for S_1 and S_4 is turned to zero. Similarly, there are 21 different OCF conditions, listed in Table II, that can be modeled.

IV. PROPOSED APPROACH FOR DETECTION AND CLASSIFICATION BETWEEN CAS AND OCFS

During various normal and abnormal operating conditions of EDS, the pure-data-driven ML schemes typically illustrate a constrained diagnosis accuracy due to varying operating conditions, nonlinear system dynamics, and weak correlation between input data features and output classes [20]. Therefore, it is always preferred to apply physics-based signal preprocessing methods on the raw data to better reflect the integrated nonlinearities of a system by incorporating the highly correlated data features. This section provides the mathematical modeling of the physics-based data features used to classify CA, OCF, and normal operating conditions of an EDS. The physics-based prior information is further integrated with an ML network to achieve better classification accuracy, referred to as the PIML approach. The presented approach comprises offline training of an ML network and its subsequent deployment in a target environment for online CPA detection as well. In this regard, the potential EDS signals used to obtain the physics-based data features are expressed as follows:

$$\mathbf{X} = \left[I_d, I_q, I_d^{\text{ref}}, I_q^{\text{ref}}, v_d, v_q, T_e, T_{\text{ipmsm}}^{\text{ref}}, \omega_m^{\text{fb}}, \omega_m^{\text{ref}}\right]. \tag{3}$$

The physics-based data features used in this study are categorized into residual- and nonresidual-based features.

A. Residual-Based Feature Acquisition

The physics-based residual features are derived to achieve stationarity for the device-level signals, as illustrated in (3). The preference for these parametric residual values stems from their characteristic of remaining within a defined range under diverse operating conditions unless an external/internal anomaly occurs; hence, they better reflect the system dynamics relevant to the mission profile of this work. Moreover, X_r^{ref},

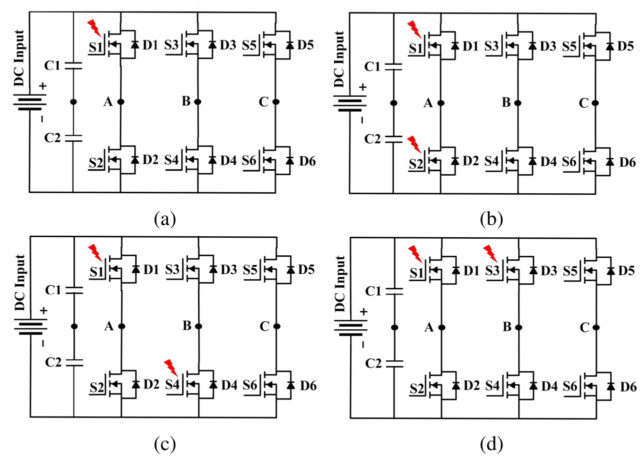


Fig. 3. Various OCF modes of inverter. (a) SS-OCF. (b) SDS-OCF. (c) CDS-OCF. (d) PDS-OCF.

referred to as tracking accuracy associated with I_d, I_q, T_e, and ω_m^{fb} at each sampling instant (k), is defined as follows:

$$X_{r(\mathrm{Id})}^{\mathrm{ref}}(k) = \left|I_d[k] - I_d^{\mathrm{ref}}[k]\right| \tag{4a}$$
$$X_{r(\mathrm{Iq})}^{\mathrm{ref}}(k) = \left|I_q[k] - I_q^{\mathrm{ref}}[k]\right| \tag{4b}$$
$$X_{r(\omega m)}^{\mathrm{ref}}(k) = \left|\omega_m^{\mathrm{fb}}[k] - \omega_m^{\mathrm{ref}}[k]\right| \tag{4c}$$
$$X_{r(\mathrm{Te})}^{\mathrm{ref}}(k) = \frac{\left|T_e[k] - T_{\mathrm{ipmsm}}^{\mathrm{ref}}[k]\right|}{\left|T_{\mathrm{ipmsm}}^{\mathrm{ref}}[k]\right| + \mu}. \tag{4d}$$

Equation (4) represents the relative error of each corresponding feedback signal with respect to its reference value, with μ as a nonnegative auxiliary variable for the case when the reference torque turns zero. Moreover, the estimated torque value and mechanical rotor speed can be calculated as follows [45]:

$$T_e[k] = \frac{3}{2}P\left[\phi_m I_q[k] + \left(L_d - L_q\right)I_d[k]I_q[k]\right] \tag{5}$$
$$\omega_m[k] = \frac{J - T_s D}{J}\omega_m[k-1] + \frac{T_s}{J}(T_e[k-1] - T_l[k-1]) \tag{6}$$

where P is the number of pole pairs, ϕ_m is the permanent magnet flux linkage, L_d and L_q are the inductance values in the dq-axis, J is the rotor inertia, D is the mechanical friction coefficient, T_s is the sampling time, and T_l is the load torque. The parameters described in (4) exhibit continuous or gradual variations during normal driving conditions, hence resulting in residual values with no abrupt response. However, in the case of detecting various abnormalities related to OCFs and CAs in EDS, these residual features illustrate a sudden response, as depicted in Fig. 4, thereby improving the classifier's performance in identifying abnormal conditions [20]. In Fig. 4, the sequence of CPAs instigated in the EDS is given in Table III. These residual-based signals mostly depict a positive correlation irrespective of various anomalies, some characterized by indistinguishable transients. In addition, when the original signals (I_{abc} and $T_{\mathrm{ipmsm}}^{\mathrm{ref}}$) are increased by only 25% using an FDI-based CA, the residual-based features illustrate either no or very minimal response, where the residual-based detection scheme may also fail. Therefore, a model-based or data-driven classifier, solely modeled based on these residual-based parameters to identify either CAs in EDS or OCFs in power switches as in [20] and [36], respectively, may fail to differentiate between these anomalies due to inadequate or homogeneous input data feature dynamics, thereby causing the misinterpretation of the system's operational states. Hence, it is crucial to introduce unique physics-based EDS features corresponding to CAs and OCFs reflecting distinctive system transients, increasing the ML classifier's generalization capabilities and reliability.

B. Nonresidual Feature Acquisition

The dynamic mathematical model of IPMSM in the synchronous rotating frame of reference is given as follows:

$$v_d = RI_d + L_d\frac{dI_d}{dt} + \omega_e L_q I_q \tag{7}$$

TABLE III

CPAs' Sequence for Figs. 4 and 7: A = {−0.75, −1.2, 1.2, 5}

OCFs	CAs (I_{abc})	CAs (ω_m^{ref})	CAs (T_{ipmsm}^{ref})
{1; 2; 7; 8; 10; 11; 16; 17}	FDI: {24; 26; 28; 31; 33; 35; 38; 40; 42; 52; 54; 56} DoS: {69, 71, 73}	FDI: {57; 58; 59; 61} DoS: {74}	FDI: {62; 63; 64; 66} DoS: {75}

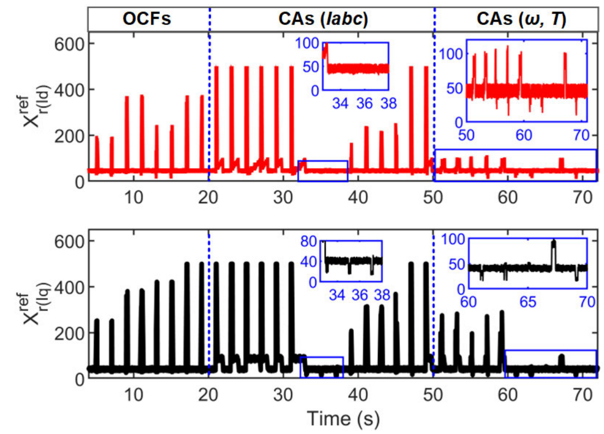


Fig. 4. Residual-based parameter's dynamics: 1000 r/min and 100 Nm.

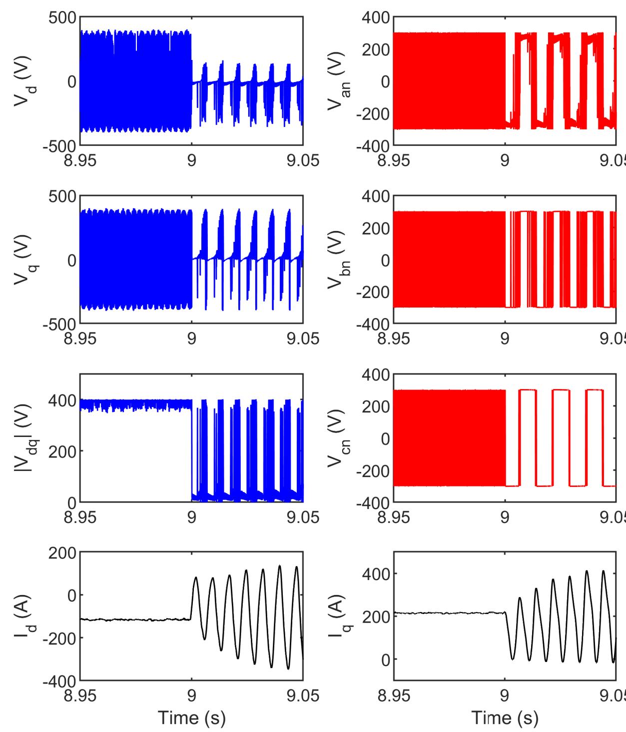


Fig. 5. Nonresidual-based parameter dynamics for SDS-OCF {7}: 1000 r/min and 100 Nm.

$$v_q = RI_q + L_q\frac{dI_q}{dt} + \omega_e L_d I_d + \omega_e\phi_m \tag{8}$$
$$\left|V_{dq}\right| = \sqrt{V_d^2 + V_q^2} \tag{9}$$

where R is the winding resistance, ω_e is electrical rotor speed in rad/s, and $|V_{dq}|$ is defined as the nonresidual physics-based feature of EDS. Moreover, (7) and (8) also account for the rate of change of I_d and I_q, which is important while distinguishing CAs and OCFs. The stator voltage values (v_d and v_q) of IPMSM are calculated based on the estimated stator current

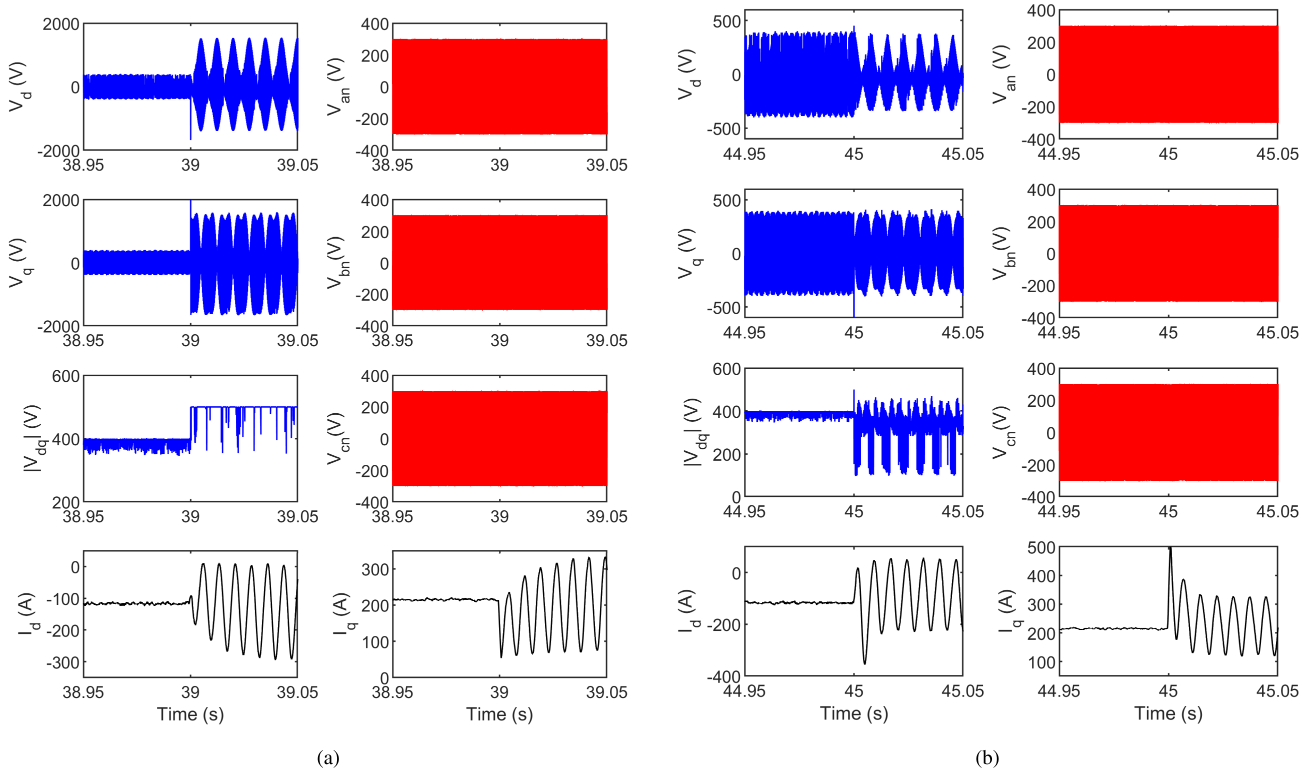


Fig. 6. Nonresidual-based parameter dynamics for CAs. (a) FDI-CA {52} and (b) DoS-CA {69}: 1000 r/min and 100 Nm.

values; thus, no additional voltage sensor is required. The v_d voltage component establishes the magnetic flux aligned with the permanent magnet's magnetic field. Meanwhile, v_q produces a magnetic field perpendicular to the rotor's field.

During normal operation under varying load conditions, the magnitude of these stator voltage components always remains balanced and within a specific boundary ($\pm 2V_{\text{dc}}/3$). However, during an OCF, the phase-to-neutral voltage drops to either $+V_{\text{dc}}/2$ or $-V_{\text{dc}}/2$, as the power switch in an associated phase can no longer connect to dc-link voltage. Hence, I_d and I_q start reducing to zero and are out of phase as one of the switches can no longer conduct, causing v_d and v_q to become zero at specific OCF instances and hence resulting in the stator voltage magnitude to fluctuate between zero and $2V_{\text{dc}}/3$, as evident in Fig. 5. Moreover, the variations in phase-to-neutral voltage due to disrupted getting signals are also illustrated in Fig. 5. Moreover, CAs result in similar fluctuations in I_d and I_q but are in phase as each switch is actually conducting, thereby producing values even higher values than $2V_{\text{dc}}/3$ for stator voltage magnitude because the direct and quadrature voltage components are no longer constraints in $\pm 2V_{\text{dc}}/3$ boundary, as illustrated in Fig. 6. In addition, an upper bound denoted as $v_{dq}^{\max}$ is assumed for stator voltage magnitude to standardize its maximum values for CAs of different intensities. Moreover, the phase-to-neutral voltage remains unaffected for attacks considered in Fig. 6. Furthermore, if we compare the results, when a DoS attack is trying to replicate the impact of SDS-OCF, residual features ($X_{r(\text{Iq})}^{\text{ref}}$) for this case are indistinguishable. However, nonresidual dq voltage components and stator voltage magnitude waveform in Fig. 5 with Fig. 6(b) illustrate a significant difference. In addition, the dynamics of the stator voltage magnitude for multiple CPAs listed in Table III are also shown in Fig. 7, showing that every OCF always illustrates a negative variance with its values never exceeding $2V_{\text{dc}}/3$. This also highlights the versatility of the proposed scheme from a data scarcity perspective, as there is no need to generate redundant data for various CPAs. Meanwhile, CAs on feedback signals of three-phase output current exhibit both positive and negative variance, producing distinguishable system dynamics. Finally, the rectified linear unit (ReLU)-based activation function logic is modified further to refine the stator voltage magnitude values for better CPA detection

$$\left|V_{dq}\right|^{+}_{(1,2,\ldots,w_s)} = \max\left(v_{dq}^{\max}, \left|V_{dq}\right|_{(1,2,\ldots,w_s)}\right)$$
$$y_{(v_{dq})} = \begin{cases} \left|V_{dq}\right|^{+}_{(1,2,\ldots,w_s)}, & \text{if } \exists i : y^{i}_{(v_{dq})} > 2V_{\text{dc}}/3 \\ \left|V_{dq}\right|_{(1,2,\ldots,w_s)}, & \text{otherwise} \end{cases} \tag{10}$$

where w_s represents the data feature window size. According to (10), if any of the values in the v_{dq} sliding window size (w_s) exceed $2V_{\text{dc}}/3$, then the values lower than $2V_{\text{dc}}/3$ will be replaced with $v_{dq}^{\max}$; otherwise, v_{dq} array will remain unchanged. Furthermore, comparing Figs. 4 and 7 shows that the CAs on the controller feedback signals have a higher impact on the system's normal operation than the reference signals. In addition, regarding FDI and DoS attacks on reference speed and torque, stator voltage magnitude in Fig. 7 displays minimal or no response for these CAs, deducing the fact that these attacks do not affect the values of direct and quadrature axis voltage components, as there is no mismatch in the feedback loop. For these cases, residual-based signals

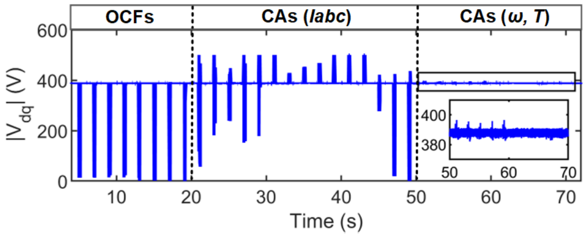


Fig. 7. Nonresidual-based parameter's dynamics: 1000 r/min and 100 Nm.

can be leveraged for CPA detection. Similarly, for the CAs with very minimal or no residual-based transient, as discussed in Section IV-A, nonresidual features show promising results for CPA detection. Hence, using both residual and nonresidual signals can enhance the detection and classification accuracy for various CPAs. Therefore, these categorical dynamics are fed into an ML classification network to distinguish between CPAs effectively.

C. CPAs' Detection Using LSTM Classifier

An LSTM is an extended version of an RNN, widely applied in various domains. In its architecture, the nodes of the RNN are replaced with a gating mechanism and memory cells [46], [47], to effectively scale the long-term dependencies of the data. Moreover, compared to conventional ML schemes, LSTM is much more effective in capturing temporal patterns and dynamic features of streaming data, making it particularly more suitable for the analysis of time-series data. Furthermore, in [20] and [48], various ML classifiers have been evaluated for PEC applications, showing that LSTM performs better compared to support vector machine, decision tree, K-nearest neighbor, naive Bayes, backpropagation neural network, radial basis function, and fuzzy neural network.

Moreover, LSTM establishes a definitive correlation among different time-series input features and better distinguishes between different system operational states. However, LSTM is computationally expensive and typically has a longer training time due to its complex architecture, as shown in Fig. 8, where the forget gate, input, and output gate are used to solve the vanishing gradient problem in conventional RNN and FNN. In addition, LSTM first calculates a candidate cell state $c'_{(t)}$ for the given input $x_{(t)}$ and output from the previous timestamp $h_{(t-1)}$, at each sampling period by using $c'_{(t)} = \tanh(m_h^c \cdot h_{(t-1)} + m_x^c \cdot x_{(t)})$. The forget gate, input gate, and output gate are calculated as follows [46]:

$$f_{(t)} = \sigma\left(m_h^f \cdot h_{(t-1)} + m_x^f \cdot x_{(t)}\right) \tag{11a}$$

$$i_{(t)} = \sigma\left(m_h^i \cdot h_{(t-1)} + m_x^i \cdot x_{(t)}\right) \tag{11b}$$

$$o_{(t)} = \sigma\left(m_h^o \cdot h_{(t-1)} + m_x^o \cdot x_{(t)}\right) \tag{11c}$$

where m_h^f, m_x^f, m_h^i, m_x^i, m_h^o, and m_x^o are the weights for each gate. Then, the new cell state $c_{(t)}$ and hidden state $h_{(t)}$ are computed by using $c_{(t)} = f_{(t)} \otimes c_{(t-1)} + i_{(t)} \otimes c'_{(t)}$ and $h_{(t)} = o_{(t)} \otimes \tanh(c_{(t)})$, respectively.

Finally, for the problem of diagnosing CPAs in EDS, the architecture of the LSTM-based multiclass classifier used in this study is shown in Fig. 9. The output of the hidden layer is passed to the output layer, where the softMax activation

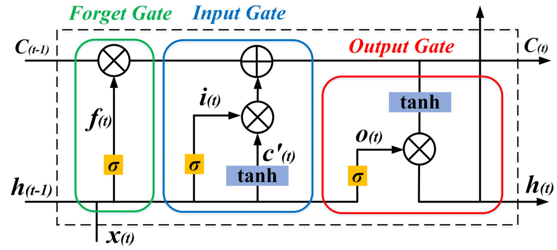


Fig. 8. Structure of a basic LSTM cell.

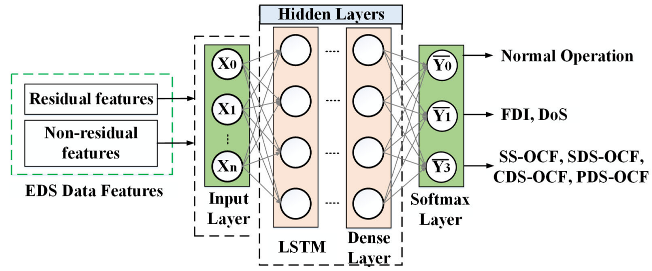


Fig. 9. General neural network architecture for CPAs' classification.

function is applied to predict the output class labels. The softmax function normalizes the output projections to a specific probability distribution with the total sum of one, which is defined as

$$\text{Softmax}(y_i(n)) = \hat{y}_i = \frac{e^{y_i(n)}}{\sum_{i=1}^{n_c} e^{x_i^{(n)}}} \tag{12}$$

where $y_i(n)$ represents the output from the dense layer's ith neuron at n learning sample and n_c is the total number of target classes. Finally, the output from softMax is fed into the categorical cross-entropy cost function to minimize the error between predicted labels and ground truth while obtaining the optimal weights for the hidden layer

$$\min\ J = H\left(y, \hat{y}\right) = -\sum_i y_i \cdot \log\left(\hat{y}_i\right) \tag{13}$$

where y_i and $\hat{y}_i$ represent the true (one-hot encoded) and the predicted probability of class i, respectively. The negative sign turns the cross-entropy minimization into a maximization problem. Finally, Tensorflow is used to build this network with hyperparameters as follows: batch size = 50, learning rate = (1 and 5 ms), hidden size = 16, and optimizer = Adam. Moreover, to estimate the performance of these ML classifiers for the proposed physics-based features, the classification accuracy can be defined as

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{14}$$

where TP represents true positives, TN represents true negatives, FP represents false positives, and FN represents false negatives. In addition, precision, recall, and F1-score are also used to examine the classifier's performance for each output class.

V. Real-Time Impact Analysis and Performance Evaluation

The performance of the proposed CPAs detection approach is demonstrated through a real-time CHIL platform setup

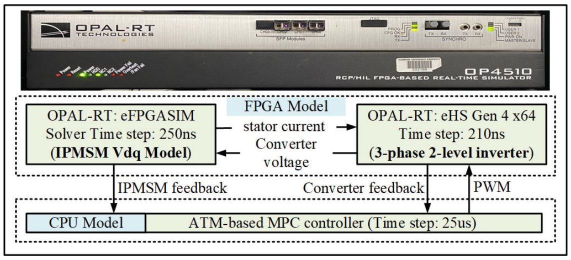


Fig. 10. EDS with ATM-based MPC control implementation on OPAL-RT testbed.

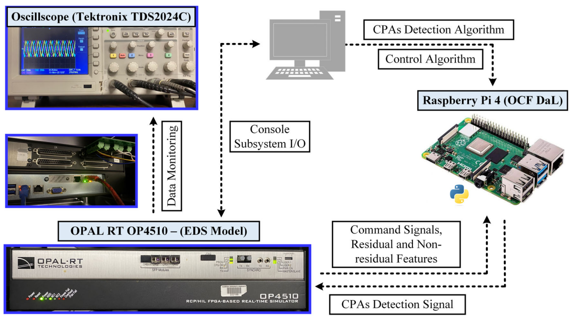


Fig. 11. CHIL experimental setup for real-time CPAs' detection.

carried out on an ATM-based MPC EDS, as shown in Fig. 2. This CHIL experiment aims to illustrate the viability of the presented framework for real-time applications. Moreover, Section V-A explains the implementation steps and experimental results for this real-time experiment.

A. System Modeling

The EDS with ATM-based MPC is implemented in MATLAB/Simulink environment integrated with the real-time digital simulator, i.e., Opal-RT OP4510. The model is executed in RT-LAB with real-time hardware synchronization mode. Moreover, the detailed implementation of EDS in OPAL-RT is shown in Fig. 10, where the power converter and IPMSM are simulated in the field-programmable gate array (FPGA) solver with a sampling time of 210 and 250 ns, respectively. The controller is implemented in the CPU of OPAL-RT with a sampling rate of 25 μs. The CPAs are instigated from the console subsystem in the real-time EDS Simulink model. Python-based scripts, such as ML multiclass classifiers, are implemented on Raspberry Pi 4 model B, which aims to detect each CPA listed in Table II and described in Section IV. The OPAL-RT and Raspberry Pi are linked via UDP. The real-time values of residual and nonresidual features from the control layer of the EDS model (i.e., OPAL-RT) are transmitted to Raspberry Pi, where an ML-based detection algorithm runs to predict output class labels based on Table II. Finally, depending upon the predicted label, a CPA detection signal is also sent back to the OPAL-RT for data monitoring on the oscilloscope. The detailed layout of the proposed CHIL experimental setup is shown in Fig. 11.

B. Real-Time Impact Analysis of CPAs on EDS Parameters

In this section, various CPAs, such as OCFs, FDI, and DoS attacks, are instigated sequentially, as listed in Table III, for detailed impact analysis on different EMT signals of the EDS.

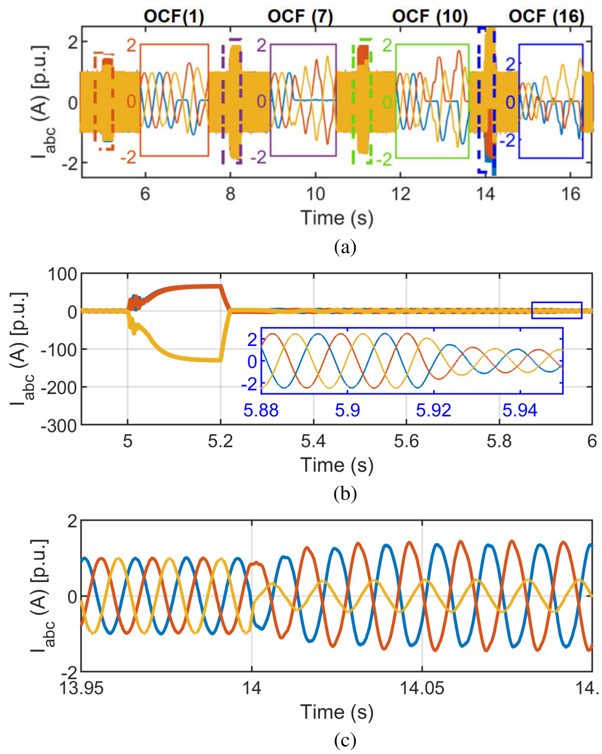


Fig. 12. Impact analysis of various CPAs on the three-phase output current: blue (Phase-A), red (Phase-B), and yellow (Phase-C). (a) OCFs {1, 7, 10, 16}. (b) FDI-CA {24}. (c) FDI-CA {52}.

1) CPAs Impact on Three-Phase Output Current: Multiple OCFs are simulated by manipulating the gate drive's switching signals, i.e., turning the gating signal of the associated power switch to zero. The impact of each category of OCFs, listed in Table II, on the three-phase output current is illustrated in Fig. 12(a). It shows that the OCF in the upper switch of a phase results in its zero positive current, and an OCF in a lower switch turns the negative current of the respective phase to zero. In addition, in the case of SDS-OCF, the overall current of the associated phase becomes zero while increasing the peak-to-peak current for the remaining phases, varying the phase shift from 120° to 180°, and impacting the IPMSM speed as well. This indicates that OCF-based physical faults impact not only the amplitude of stator current but also frequency and phase, which can be further analyzed by using the FFT analysis. Moreover, these current signals can also be tempered by a smart attacker hijacking the CAN or LIN communication framework associated with the current sensor block. In this context, Fig. 12(b) and (c) shows the impact of FDI-based CA on three-phase output current, showing that the FDI attack with $A < 0$ has a more severe impact compared to the case where $A > 0$. These FDI-based CAs cause the magnitude values of I_d and I_q, feeding into the controller, to vary while disrupting the controller's MPC algorithm to produce distinct impacts on IPMSM stator currents.

2) CPAs Impact on dq-Axis Stator Current, Speed, and Torque: CPAs can interfere with the EDS's normal operation at different levels. However, it is not always true that OCF-based physical faults have a higher impact than CAs. Therefore, to investigate EDS response further, multiple CPAs listed in Table III are instigated sequentially. In this regard,

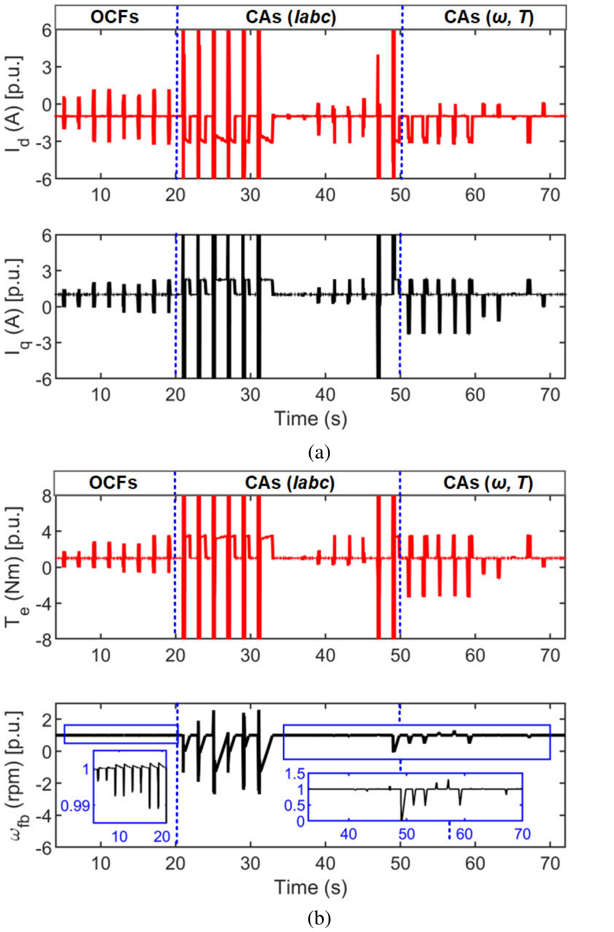


Fig. 13. Impact analysis of various CPAs (following Table III sequence). (a) Electrical parameters. (b) Mechanical parameters.

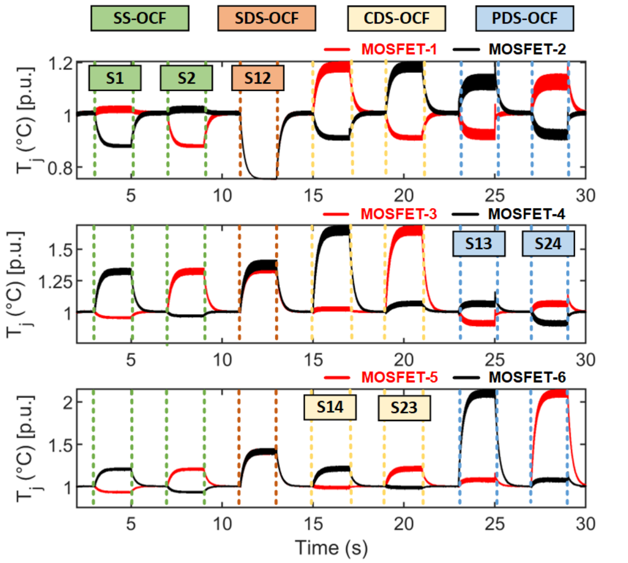


Fig. 14. Impact analysis on the junction temperature of each MOSFET for various OCFs.

Fig. 13 shows that the FDI-based CAs with $A <= 0$ are among the high-intensity attacks. Moreover, for the FDI-based CAs, where the values for I_{abc} and $T_{\text{ipmsm}}^{\text{ref}}$ are increased by only 25%, there is no substantial impact on either the electrical or mechanical parameters of EDS. The same can also be seen in residual-based features, as shown in Fig. 4. Furthermore, in the case of OCFs, PDS-OCF seems to have the highest impact among other categories of OCFs. In addition, FDI and DoS-based CAs on $T_{\text{ipmsm}}^{\text{ref}}$ do not have a major impact on the EDS performance. However, these types of attacks can indirectly impact the discharging and degradation rate of the battery by exerting high load torque values, which can be a promising area of research to explore. As the electrical properties of the EDS transfer the same effect on mechanical characteristics, the impact analysis implications are the same for each CPA discussed above. Moreover, these CPAs also impact the IPMSM speed, showing that EDS fundamental frequency can also be influenced via these anomalies. Therefore, a detailed harmonic analysis of these waveforms via FFT or wavelet analysis can also be done in the frequency domain for harmonics-based CA detection and classification, which is part of our future work.

3) CPAs' Impact on MOSFET's Junction Temperature: In this study, the variations in the stator currents due to various CPAs are reflected in the form of varying conduction losses in the power switch and antiparallel diode, which are further used to calculate the junction temperature (T_j) of each MOSFET. In this regard, the ambient temperature is considered to be 49 °C, and for the reference speed of 1000 r/min and the load torque of 100 Nm, T_j increases to 65 °C during regular operation of the inverter. Moreover, Fig. 14 shows the normalized values of T_j associated with each MOSFET under various categories of OCFs in EDS. In the case of SS-OCF, the impact on T_j of the switch under fault is not much because the conduction losses of the associated antiparallel diode have increased due to higher negative or positive half current. However, the losses in at least two of the MOSFETs in the remaining phases have risen due to high phase current, hence increasing the associated T_j. In addition, for SDS-OCF, T_j for both MOSFETs has dropped to ambient temperature, i.e., almost 75% of the nominal T_j, because the associated phase current has become zero. However, T_j for the rest of MOSFETs has increased in a homogeneous pattern due to their similar dynamics of stator currents, as shown in Fig. 12(a). Furthermore, in the case of CDS-OCF, each MOSFET under fault experiences the highest values of T_j due to increased stator currents in respective phases. Meanwhile, in the case of PDS-OCF illustrated in Fig. 14, one of the MOSFETs in the nonfaulty phase illustrates the highest T_j. These variations in T_j for each MOSFET ($S1, S2, \ldots, S6$) during various OCF categories are listed in Table IV, showing that the CDS-OCFs and PDS-OCFs cause the highest active and passive thermal stress on MOSFETs, respectively. Moreover, the MOSFETs with the highest T_j are also highlighted.

In the case of CAs, the controller's reference and feedback signals are maliciously modified, which in real-world operation can also further impact each MOSFET's T_j. The variations in T_j for these semiconductor devices are proportional to their conduction current. In this regard, the effect of FDI-based CA (52) on the three-phase stator currents is shown in Fig. 12. As a result, the output current for phases A and B is increased, and for phase C, it is reduced. Therefore, T_j for MOSFETs in phases A and B is higher than for phase C,

TABLE IV
THERMAL STRESS ON MOSFETs UNDER VARIOUS CPAs

Operation Modes	Junction Temperature (°C) [p.u.]					
	M1	**M2**	**M3**	**M4**	**M5**	**M6**
SS-OCF (1)	1.02	0.87	0.95	1.33	0.92	**1.21**
SS-OCF (2)	0.87	1.02	1.33	0.95	**1.21**	0.92
SDS-OCF (7)	0.75	0.75	1.37	1.35	**1.41**	**1.41**
CDS-OCF (10)	1.18	0.91	1.03	**1.65**	0.99	1.20
CDS-OCF (11)	0.90	1.18	**1.65**	1.08	1.20	0.98
PDS-OCF (16)	0.91	1.11	0.91	1.07	1.06	**2.1**
PDS-OCF (17)	1.11	0.91	1.05	0.90	**2.1**	1.07
FDI: Ic (52)	**1.18**	**1.18**	**1.18**	**1.18**	0.83	0.83
FDI: Ibc (54)	**1.01**	**1.01**	0.88	0.88	0.88	0.88
FDI: Iabc (56)	0.84	0.84	0.84	0.84	0.84	0.84
DoS: Ic (69)	0.98	0.98	0.92	0.92	**1.22**	**1.22**
FDI: T_{ipmsm}^{ref} (61)	1.92	1.92	1.92	1.92	1.92	1.92
FDI: ω_m^{ref} (66)	1.00	1.00	1.00	1.00	1.00	1.00

TABLE V
NUMBER OF DATA POINTS FOR EACH OUTPUT CLASS

Output Classes (label)	No. of Data Points
Normal Operation (0)	55,028
Open Circuit Faults (1)	55,028
Cyber Attacks (2)	55,028

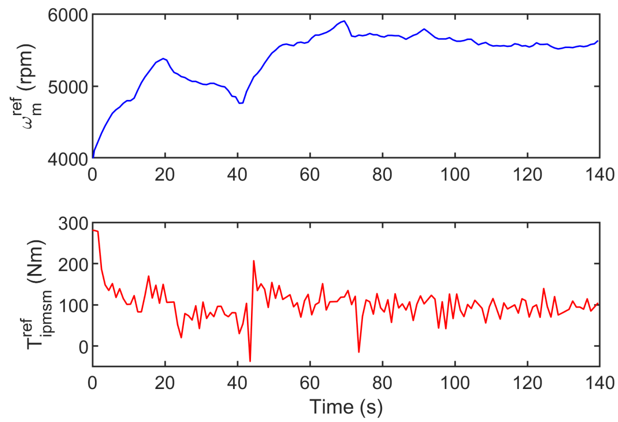


Fig. 15. Reference speed and torque profile used for training data acquisition.

TABLE VI
PEARSON CORRELATION COEFFICIENTS FOR THE TRAINING DATASET

EDS Input Data Features	Output Classes		
	Normal Operation	**Open Circuit Fault**	**Cyber Attack**
$X_{r(Id)}^{ref}$	-0.255	-0.122	0.404
$X_{r(Iq)}^{ref}$	-0.386	0.029	0.434
$\lvert V_{dq}\rvert$	**0.131**	**-0.778**	**0.453**

as listed in Table IV. Similarly, when this FDI-based CA is further extended to phases A and B, their associated stator currents also reduce, similar to phase C. Therefore, T_j is decreased for all six MOSFETs, as shown for FDI-based CA (56). On the contrary, for the DoS attack on phase C current (69), T_j increases for M5 and M6 because the CAs with $A <= 0$ tend to elevate the phase current. Moreover, in the case of CA on $T_{\text{ipmsm}}^{\text{ref}}$, the reference torque for EDS has been increased maliciously, consequently elevating the three-phase output current evenly and hence increasing T_j for each MOSFET. Therefore, through this attack, an adversary can not only rapidly deplete the battery but also escalate the thermal stress on power switches while potentially resulting in an OCF. Furthermore, in the scenario of a CA on reference speed, T_j remains unaffected for all MOSFETs because ω_m^{ref} solely influences the fundamental period of the three-phase current, not its magnitude. Hence, this analysis shows that these CPAs can also impact the device-level characteristics of an EDS and can result in severe or permanent damage to the system components.

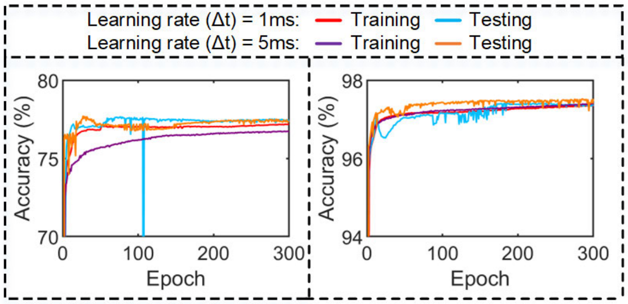
C. Real-Time Training Data Acquisition

To validate the performance and reliability of the proposed PIML approach for CPA detection for real-time system dynamics, training data are acquired from the OPAL-RT-based EDS model illustrated in Fig. 10. Moreover, to realize the real-world dynamics of reference signals, varying speed and load torque profiles are employed during the training data acquisition from the EDS model, as depicted in Fig. 15. Various OCFs and CAs are instigated sequentially at different instants, ensuring that each set of normal operation time-series data points is followed by either an OCF or CA dataset. This approach allows us to capture the transient response from the onset of each event. Real-time data for both residual and nonresidual EDS features are gathered across all 75 operating modes (as listed in Table II) and stored in a.mat file using the Opwrite block in Simulink. The dataset is composed of three distinct classes: normal operation, OCFs, and CAs. The overall composition of the training data, including the number of data points associated with each output class, is detailed in Table V.

The number of data points can vary for each class, reflecting the rate of occurrence of each operational mode in the simulated environment. However, to achieve an unbiased, accurate, and reliable model, the dataset is balanced by ensuring an equal number of data points in each class. The data points associated with residual features are homogeneous, both within and across classes. However, the nonresidual features are homogeneous within each class but heterogeneous among different classes, hence ensuring consistency within each class and discrimination among classes. Moreover, the Pearson correlation coefficients are calculated between each input feature and the target variable to evaluate the training dataset's applicability and to reduce multicollinearity. The features with the highest Pearson correlation coefficient values relative to the target variables are listed in Table VI, showing that the nonresidual feature is strongly correlated with output labels.

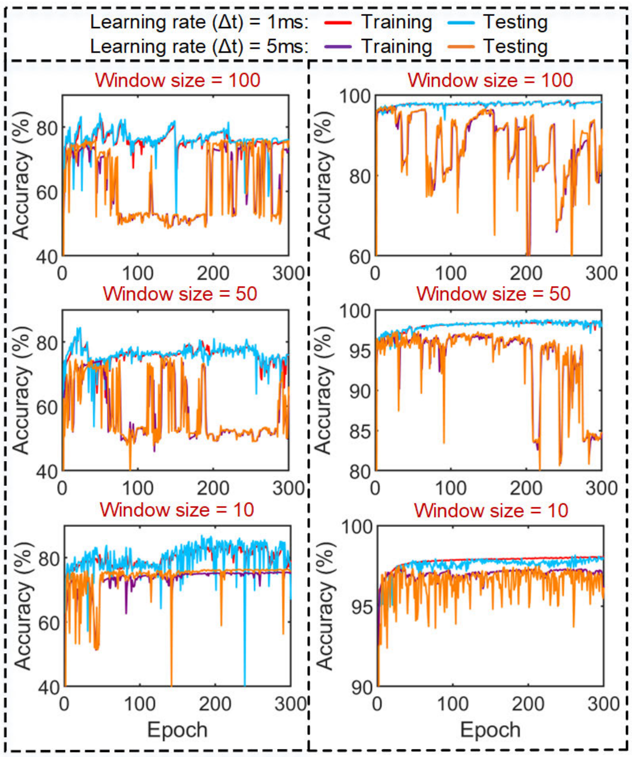
D. Offline Training and ML Model Selection

The acquired EDS data are split into training and testing datasets with a 70:30 ratio. This dataset is subsequently utilized to train and evaluate various ML networks, including FNN, RNN, and LSTM. Moreover, the architecture of the LSTM-based neural network is already explained in Section IV. For other ML classifiers, only the first hidden layer in the LSTM-based network's architecture is replaced with a dense layer and RNN, thus transforming it into an FNN and RNN-based classifier. The training parameters of these ML networks can directly impact their performance [49].



(a) (b)

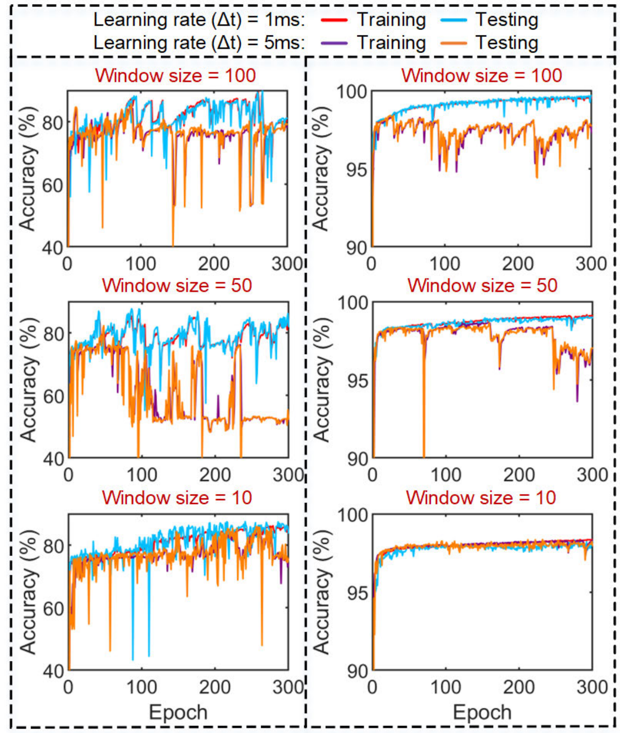
Fig. 16. Accuracy curves in the training process for FNN-based classifier. (a) Residual-based features [20]. (b) Residual and nonresidual features (proposed).



(a) (b)

Fig. 17. Accuracy curves in the training process for RNN-based classifier. (a) Residual-based features [20]. (b) Residual and nonresidual features (proposed).

In this regard, the batch size, defined as the number of data samples that the ML model needs to go through before changing its internal parameters, has a substantial impact on the training time and model accuracy. The larger batch size results in fast training but, however, may lead to low accuracy and overfitting, whereas the smaller batch size can be computationally expensive but might yield higher accuracy. Moreover, regarding learning rate, a higher value is typically preferred as it can lead to faster model convergence; however, if the value is too high, it can also cause the model to diverge as well, whereas a smaller learning rate can result in precise convergence but will require more iterations. Moreover, the window size (ω_s) can directly impact the detection time of the proposed approach, and hence, it is preferred to choose a smaller window size with higher classification accuracy. These hyperparameters are optimized to achieve fast convergence,



(a) (b)

Fig. 18. Accuracy curves in the training process for LSTM-based classifier. (a) Residual-based features [20]. (b) Residual and nonresidual features (proposed).

TABLE VII

PERFORMANCE EVALUATION OF VARIOUS ML CLASSIFIERS

ML Classifiers	Output Labels	P	R	F1	Acc (%) [Train, Test]
FNN Δt = 5ms	0	0.96	0.99	0.98	[97.52, 97.40]
	1	1.00	0.98	0.99	
	2	0.98	0.95	0.97	
RNN Δt = 1ms ω_s = 100	0	0.97	1.00	0.98	[98.46, 98.43]
	1	1.00	1.00	1.00	
	2	0.99	0.96	0.98	
LSTM Δt = 5ms ω_s = 100	0	0.99	1.00	1.00	[99.68, 99.57]
	1	1.00	1.00	1.00	
	2	1.00	0.99	1.00	

better fitting, and higher accuracy for training and testing datasets. Moreover, the ML network structures are kept as simplistic as possible to mitigate the computational as well.

For performance evaluation, Fig. 16 signifies the FNN classifier's accuracy rate for two different input datasets while considering different learning rates for 300 epochs. Notably, the FNN demonstrates superior classification accuracy for the proposed EDS's feature extraction approach at the learning rate of 5 ms. In addition, Figs. 17 and 18 illustrate the accuracy of RNN and LSTM-based multiclass classifiers, respectively. Their performance is evaluated across various window sizes (w_s) and learning rates over 300 epochs, revealing that LSTM exhibits superior accuracy compared to all other ML classifiers at $w_s = 100$. Generally, a shorter feature extraction window size is favored due to its potential to decrease detection time. However, this choice may also reduce the ML classifier's accuracy, as evident in Figs. 17 and 18. Finally, the classification performance metrics, including precision, recall, F1-score,

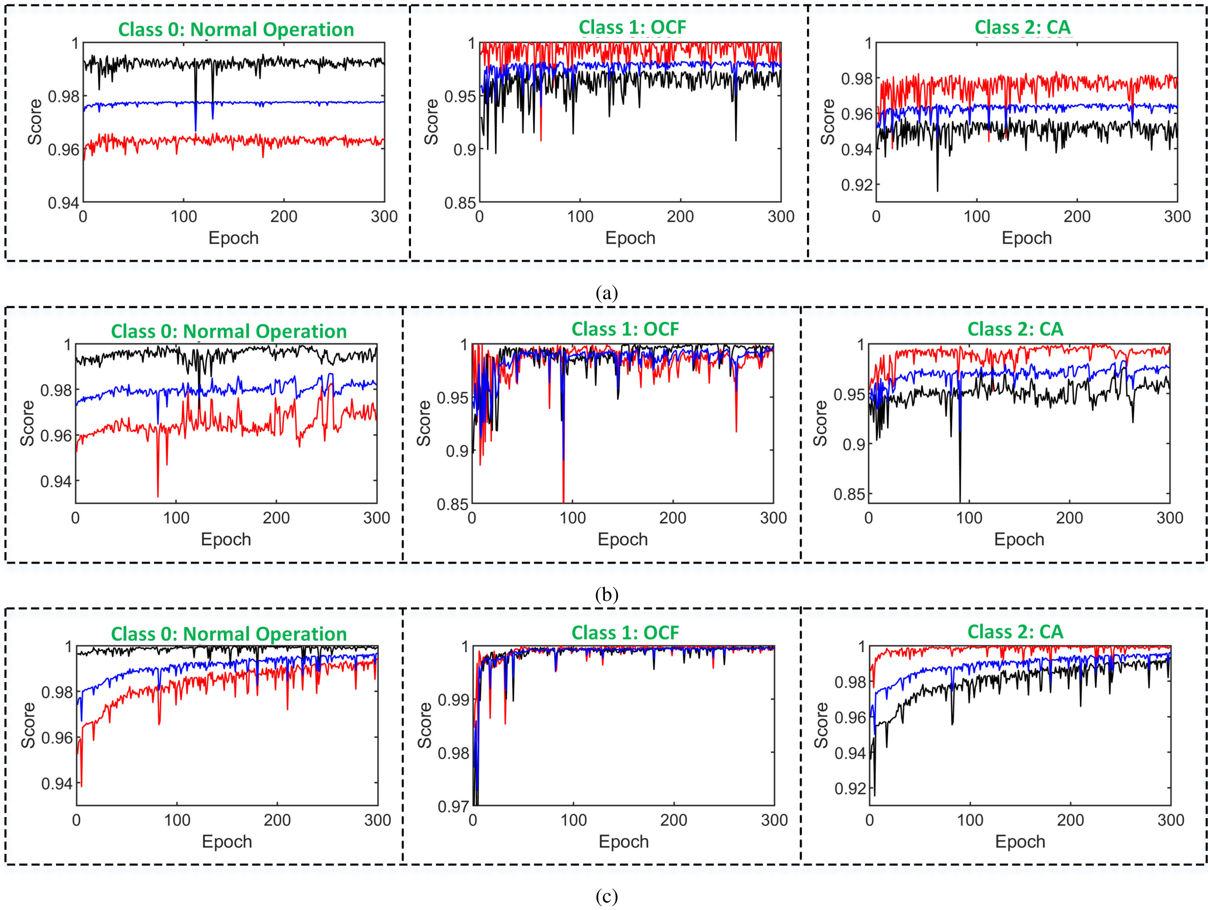


Fig. 19. Precision (red), recall (black), and F1-score (blue) evolution over the training epochs. (a) FNN. (b) RNN. (c) LSTM.

TABLE VIII
LSTM HYPERPARAMETERS

Hyperparameter	**Value**
Number of epochs	300
Learning rate (Δt)	0.001
Window size (ω_s)	100
Batch size	50
Input dimensions	(100,5)
Number of layers	5
Activation function	ReLU
Optimizer	Adam
Weight initialization	42
Dropout rate	0.2

TABLE IX
LSTM CLASSIFIER'S ARCHITECTURE

Layers
LSTM(input_size= (100,5), hidden_size=16, num_layers=1, batch_first=True, return_sequences = False)
Dropout(0.2)
Linear(16, 16)
Dropout(0.2)
Linear(16, 3)

and accuracy, are used to select the best ML model and its associated hyperparameters, as summarized in Table VII. Moreover, the evolution of precision, recall, and F1-score over the training epochs for the ML model depicted in Table VII is also illustrated in Fig. 19. Notably, the LSTM-based ML classifier shows the highest performance metrics values for the proposed PIML approach. The associated hyperparameters and architecture of this LSTM network are illustrated in Table VIII and IX, respectively.

E. CPAs Intensity-I: Offline Diagnosis of CPAs for US06 Drive Cycle

To validate the performance of the proposed PIML approach using an LSTM-based classifier, the trained model is subjected to offline testing using the US06 drive cycle. The sequence of various CPAs instigated at different time intervals of this drive cycle is presented in Table X. Moreover, the general layout of the training and validation framework is shown in Fig. 20. In this case, the intensity of CPAs is regarded as minimal as only SS-OCFs and FDI-based CAs subjected to only single-phase output current are considered. However, as a result of these anomalies, the transients of various EDS features exhibiting varying amplitudes based on different driving conditions are shown in Fig. 21. Most of the residual-based features indicate a positive variance concerning different CPAs, which makes it hard for a simple classification scheme to distinguish between a CA and an OCF, as discussed in Section IV. However, the values for the magnitude of stator current show a positive variance for cyberattacks and a negative variance for OCFs. To make this proposition more robust, OCFs are introduced in all six MOSFETs individually,

TABLE X

CPAs Sequence for US06 Drive Cycle Case-I (Time Span = 3 s)

No.	Target	t_{cpa}	No.	Target	t_{cpa}
1	S4	24	9	S1, S5	330
2	Ic {A=-0.75}	70	10	Ibc {A= -1.2}	393
3	ω_m^{ref} {A=-1.2}	97	11	$Iabc$ {A= 5}	461
4	Ic {A=0}	112	12	Ia {A=0}	483
5	ω_m^{ref} {A=0}	135	13	S1, S4	500
6	S4, S5	164	14	Ia {A= 1.2}	550
7	S3, S4	228	15	ω_m^{ref} {A=2}	575
8	T_{ipmsm}^{ref} {A=5}	292			

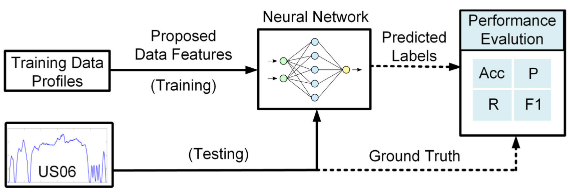


Fig. 20. Performance evaluation of the ML classifiers.

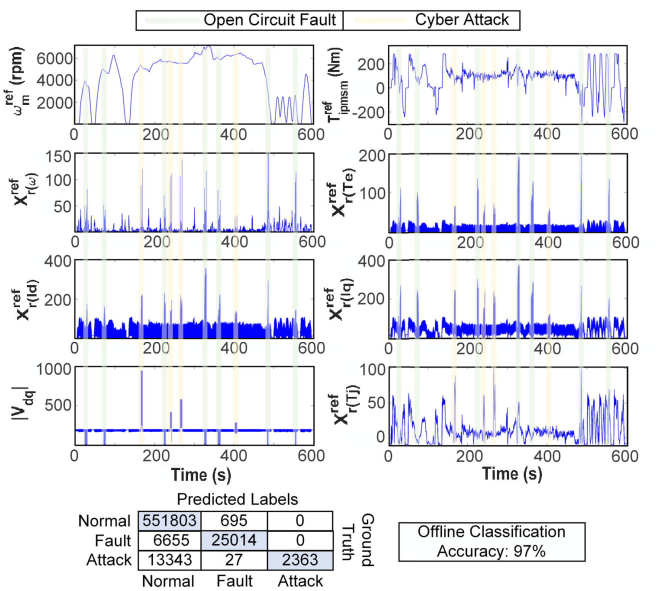


Fig. 21. CPAs detection in EDS for US06 drive cycle, offline diagnosis (Table X).

along with CAs of different intensities, on various time stamps and randomly. Hence, the performance of the proposed PIML-based CPA diagnosis scheme is tested, which results in a classification accuracy of 97%, as represented in the form of the associated confusion matrix shown in Fig. 21. Moreover, this accuracy may be further increased by using a more sophisticated motor control framework with lesser total harmonic distortions or a real-time controller with high-speed computational power.

F. CPAs' Intensity-II: Real-Time CHIL Online Diagnosis of CPAs for US06 Drive Cycle

In order to further substantiate the practical applicability of the proposed approach, various CPA scenarios from Table II are implemented via the CHIL experimental setup shown in Fig. 11. The real-time output labels are derived from the LSTM classifier operating in real time on the Raspberry Pi. Moreover, the CPAs instigated at different instances of the

TABLE XI

CPAs' Sequence for US06 Drive Cycle Case-II (Time Span = 3 s)

No.	Target	t_{cpa}	No.	Target	t_{cpa}
1	S3	20	7	S5	330
2	S4	80	8	S2	360
3	Ia {A=5}	170	9	Ic {A=1.5}	410
4	S1	220	10	S6	490
5	Ia {A=2}	230	11	S1	570
6	Ib {A=3}	255			

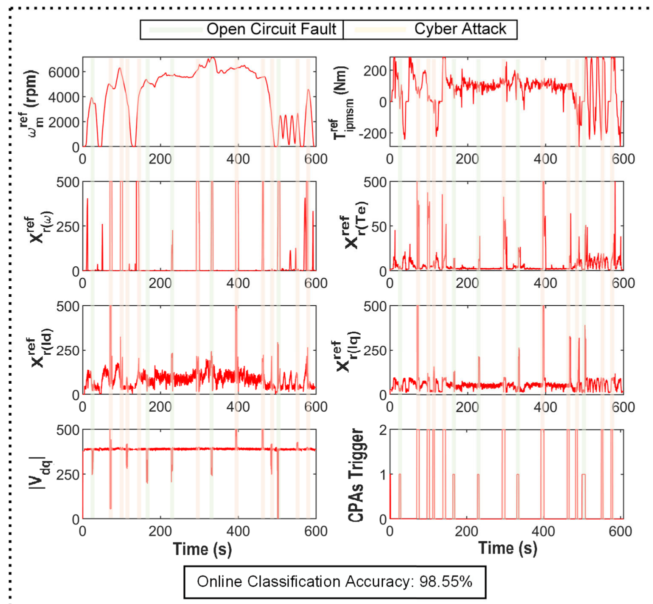


Fig. 22. CPAs' detection in EDS via CHIL experiment for US06 drive cycle, online diagnosis (Table XI).

US06 drive cycle are listed in Table XI. In order to mitigate the fluctuations in EDS data, the rolling mean is applied to the real-time test dataset of size ω_s, obtained from OPAL-RT, thereby reducing the probability of false alarms. The transients of various real-time EDS signals used for system state prediction are shown in Fig. 22. In addition, the real-time values of the corresponding CPA's trigger signal (output label) are also depicted in Fig. 22. The accuracy for the real-time detection is 98.92%, which is significantly increased compared to offline detection, mainly due to the utilization of a refined test dataset obtained by applying the rolling mean approach. Moreover, the accuracy in real-time is derived by comparing the feedback CPA trigger values received from Raspberry Pi with the ground truth labels in OPAL-RT. Therefore, the accuracy decreases if there is a mismatch between predicted and actual labels. In this regard, there are one of two main reasons for this mismatch: 1) when the CPA is disabled from the console block in Simulink, the EDS test dataset features still have some inertia and they do not turn back to their normal response abruptly, thus prolonging the OCF or CA label and 2) the delayed diagnosis caused by communication and computation delays also causes this mismatch before and after the instigation of a CPA.

G. Detection Time Analysis of the Proposed Approach

The real-time data acquisition results, related to the three-phase output current and CPA trigger signal, are displayed by using an oscilloscope (Tektronix TDS2024C) connected to the analog output port of OPAL-RT. CH1, CH2, and CH3 correspond to phase-A, phase-B, and phase-C currents, respectively, while CH4 represents the predicted target labels associated with each system state listed in Table II. Moreover, there is always a system delay during online diagnosis, resulting in false alarms from delayed detection, and hence reducing the overall accuracy. In this context, the total detection time of EDS's various operating states can be represented as follows:

$$T_{\text{det}} = T_{\text{ws}}^{d} + T_{\text{com}}^{d} + T_{\text{compu}}^{d} \tag{15}$$

where T_{ws}^{d} represents the delay associated with the required time to gather EDS test dataset features equal to the window size, T_{com}^{d} is the communication delay associated with the UDP framework, and T_{compu}^{d} is the computational delay corresponding to the LSTM-based ML classifier. T_{com}^{d} and T_{compu}^{d} can be associated with the system delay. Moreover, based on the theoretical analysis, for the controller's sampling period of 25 μs and $w_s = 100$, the value of T_{ws}^{d} will be 2.5 ms, which is the actual detection time of the proposed approach. However, the communication and computational delays can vary depending on the data transmission rate of the communication framework and computational resources at hand. In this regard, Fig. 23 illustrates the real-time detection delay for various CPA scenarios related to the proposed approach, implemented via the CHIL experimental setup shown in Fig. 11. Therefore, based on the results in Fig. 23, the average detection time is 75 ms, where 2.5 ms corresponds to T_{ws}^{d}, and the remaining time is associated with communication and computational delay. Hence, due to this system delay affecting all CPAs in the US06 drive cycle, false alarms occur in approximately 0.37% of the total data samples. Therefore, if we assume an ideal system with zero system delay, the real-time accuracy of our proposed approach can pushed up to 98.92%.

Hence, the proposed physics-based features can effectively extract the system dynamics related to abnormal conditions, which can be further used for CPA detection and classification for practical scenarios. The accuracy of CPA diagnosis for an actual drive cycle can be degraded based on different driving conditions and system-level computational limitations. In this regard, the majority vote mechanism can also be utilized to reduce the probability of false alarms associated with real-world operating conditions.

H. Comparative Analysis With Prior Studies

Finally, a comparative analysis of this study with various past studies that employed data-driven approaches, such as LSTM, residual-based methods for PIML, transfer learning, and data preprocessing with binary classifiers, for the cyber–physical security of EDS, is summarized in Table XII. The proposed approach has a major advantage compared to residual-based schemes [20], which are inherently susceptible to misidentifying both cyber or physical anomalies in a system. Moreover, this study is also compared with the ML schemes using EDA and FFT as feature's data preprocessing schemes [16], [19], [24] to improve the detection accuracy.

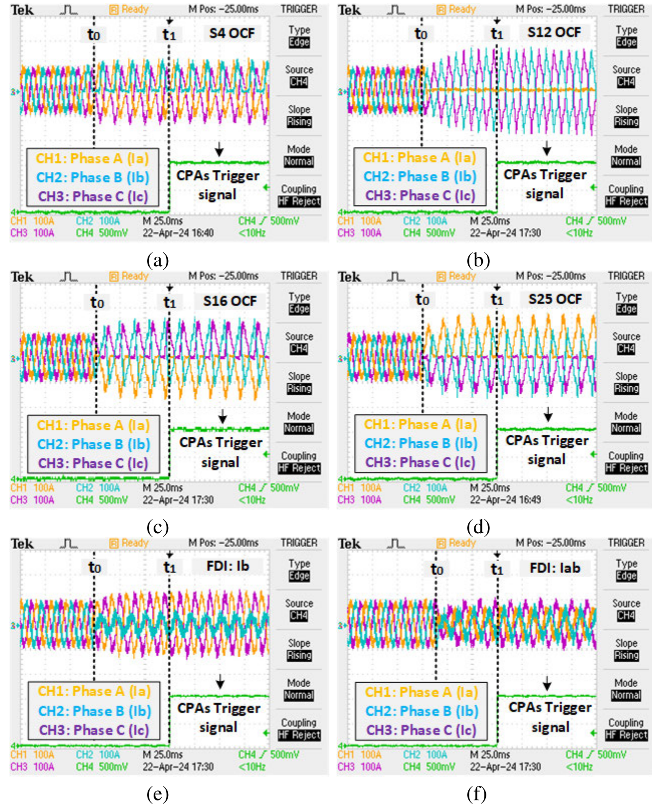


Fig. 23. CHIL-based online CPA diagnosis showcasing detection and system delay. (a) SS-OCF (4). (b) SDS-OCF (7). (c) CDS-OCF (14). (d) PDS-OCF (15). (e) FDI-CA (51). (f) FDI-CA (53).

The comparison reveals that the proposed approach exhibits superior detection speed and accuracy. Moreover, in the case of the transfer learning scheme [15], [50], which has significant benefits for limited experimental data and results in high accuracy for FDI-based CAs detection, however, its detection time is considerably longer compared to the proposed approach. Moreover, the accuracy of the schemes that did not use any practical drive cycle with real-time driving conditions as testing data may not be reliable. Hence, the presented study is unique as it can differentiate between the most common OCF-based physical fault and FDI or DoS-based CA, achieving faster detection times and higher accuracy, which has not been addressed in any previous work. Moreover, the proposed schemes also investigate the thermal impact analysis of various CPAs on MOSFETs along with the electrical and mechanical parameters of EDS, which to the best of our knowledge has also not been explored in the existing literature.

I. Preliminary Discussion on Distinguishing Common Current Sensor Faults

Despite the highest reliability scores attributed to current sensors in EDS [5], [6], they remain vulnerable to physical faults and performance degradation. This vulnerability can impact the performance of both the EDS controller and the associated diagnostic algorithm. Common current sensor faults encompass stuck faults, offset faults, and noise faults [24]. The impact of these faults on the three-phase output current is illustrated in Fig. 24. Stuck and offset faults significantly impact EDS control parameters, leading to false alarms due to

TABLE XII
PROPOSED RESEARCH CONTRIBUTION COMPARISON WITH PRIOR RESEARCH STUDIES SUBJECT TO ANOMALY DETECTION

Research Methodology	Model Characteristics				
	CA Detection	OCF Detection	TIA	Detection Time	Accuracy (Drive Cycle)
LSTM-based approach [51]	T	NT	NT	- -	92.10% (None)
Transfer learning with CNNs [15]	T	NT	NT	50.0ms	99.50% (None)
Transferable data-driven approach [50]	NT	T	NT	40.0ms	88.53% (None)
FFT with RVFL neural network [24]	NT	T	NT	20.0ms	98.83% (None)
EDA with random forest [19]	T	NT	NT	12.5ms	99.90% (NEDC)
FFT with random forest [16]	T	NT	NT	10.0ms	90.00% (None)
Residual feature-based PIML [20]	T	NT	NT	2.5ms	98.44% (UDDS)
Proposed Approach	T	T	T	2.5ms	98.92% (US06)

TIA (Thermal Impact Analysis). NT (Not Tested). T (Tested). UDDS (Urban Dynamometer Driving Schedule). NEDC (New European Driving Cycle). EDA (Exploratory Data Analysis).

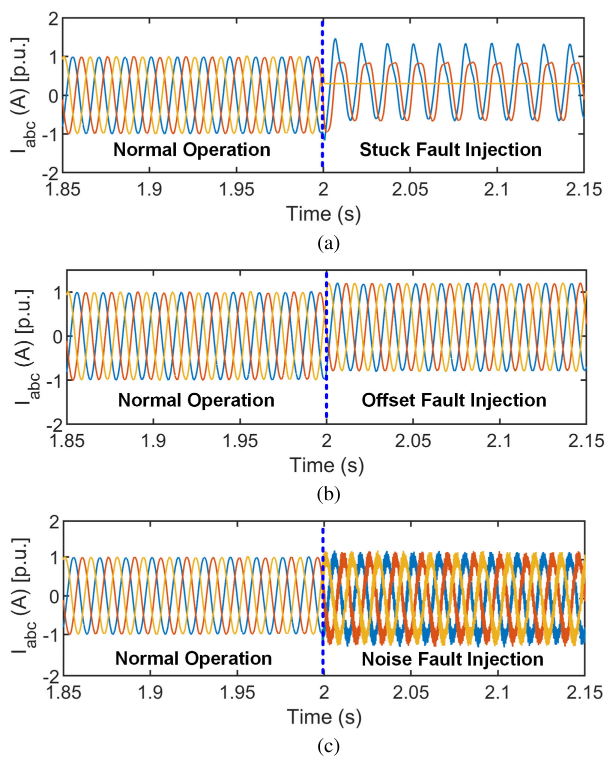


Fig. 24. Impact analysis of current sensor faults on the three-phase output current: blue (Phase-A), red (Phase-B), and yellow (Phase-C).

overlapping residual and nonresidual diagnostic features with those of CAs. In contrast, noise faults mainly cause increased total harmonic distortion in the stator current, leading to reduced power quality and increased torque ripples. Therefore, stuck and offset faults are critical concerns that should be addressed in a diagnostic algorithm. Since the proposed PIML approach mainly focuses on detecting and distinguishing OCFs and CAs, developing a new method to handle sensor faults is necessary and presents a promising open research question.

The distinctions in three-phase currents due to CAs, power switch-based OCF faults, and current sensor faults can be observed in Figs. 12 and 24. To enable an ML-based multiclass classifier to accurately differentiate between these nonroutine system states, the diagnostic features must exhibit heterogeneity across each output class. However, the proposed physics-based features fall short of providing those distinctive features for current sensor fault isolation. To address this, further filtering of three-phase current data using frequency-domain analysis could be advantageous, which is the focus of our future work. In addition, developing an energy-based evaluation criterion, independent of the unified PIML approach, could also assess the operational state of current sensors more accurately. EVs can monitor this energy consumption by accessing these sensor nodes [52]. A defective sensor node often consumes an abnormal amount of energy, either more or less than its specified value, leading to unreliable outputs. By monitoring the sensor's energy consumption, we can assess its performance and identify potential faults. Thus, this energy-based evaluation criterion can be formulated as follows:

$$\mathrm{Tgr}_{(sf)} = \begin{cases} 1, & |E_s(t) - E_{\text{rated}}| \geq E_{\min} \\ 0, & \text{otherwise.} \end{cases} \quad (16)$$

This suggests that when a sensor's energy consumption deviates from the specified tolerance threshold, it indicates a malfunction in its normal operation. This aspect will be thoroughly explored in our subsequent research work.

VI. CONCLUSION

This study presents a PIML approach to distinguish between normal and abnormal operations of EDS, focusing on common CAs affecting reference and feedback signals, as well as OCFs in power switches. In this regard, novel physics-based stator voltage features are utilized along with residual-based features for the classification of CPAs. The impact of various CPAs on EDS's EMT characteristics is also analyzed. The proposed methodology is validated offline for various ML models, showing that LSTM has the highest classification accuracy. Moreover, to authenticate the practical feasibility of the proposed study in real-time scenarios, CPAs are detected online for the US06 drive cycle via the CHIL experimental setup, demonstrating an accuracy of 98.92%. Moreover, this study includes consideration of FDI and DoS attacks, as they are among the most frequently discussed CAs in previously published literature. However, the future focus of this study will incorporate replay attacks as well. The presented approach can provide reliable detection signals to the subsequent countermeasure control. Therefore, for a resilient EDS operation, a secondary layer with novel mitigation schemes for CAs and OCFs will also be proposed as a future part of this work.

ACKNOWLEDGMENT

This study was supported by the Simulation-Based Reliability and Safety Program for modeling and simulation of military ground vehicle systems, under the technical services contract No. W56HZV-17-C-0095 with the U.S. Army DEVCOM Ground Vehicle Systems Center (GVSC). DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited. (OPSEC 7856). The authors would like to express their gratitude for the valuable resources and facilities provided by the Secure Energy and Automation Laboratory (SEAL) and Real Time Controls and Optimization Laboratory (RTCOOL). The authors would like to acknowledge the Warren H. Owen Distinguished Professorship Endowment for its support of the research effort.

REFERENCES

[1] *Global Automotive Cybersecurity Report 2023*. Accessed: May 28, 2024. [Online]. Available: https://upstream.auto/reports/global-automotive-cybersecurity-report/

[2] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Impact analysis of data integrity attacks on power electronics and electric drives," in *Proc. IEEE Transp. Electrific. Conf. Expo (ITEC)*, Jun. 2019, pp. 1–6.

[3] J. Ye et al., "Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 4, pp. 4639–4657, Aug. 2021.

[4] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Vulnerability assessments of electric drive systems due to sensor data integrity attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3301–3310, May 2020.

[5] L. Julian and G. Oriti, "A comparison of redundant inverter topologies to improve voltage source inverter reliability," *IEEE Trans. Ind. Appl.*, vol. 43, no. 5, pp. 1371–1378, Sep./Oct. 2007.

[6] R.-D. Klug and M. Griggs, "Reliability and availability of megawatt drive concepts," in *Proc. Int. Conf. Power Syst. Technol., PowerCon.*, vol. 1, 2004, pp. 665–671.

[7] X. Zhou, J. Sun, H. Li, M. Lu, and F. Zeng, "PMSM open-phase fault-tolerant control strategy based on four-leg inverter," *IEEE Trans. Power Electron.*, vol. 35, no. 3, pp. 2799–2808, Mar. 2020.

[8] J. Giraldo et al., "A survey of physics-based attack detection in cyber-physical systems," *ACM Comput. Surv.*, vol. 51, no. 4, pp. 1–36, Jul. 2019.

[9] S. Mishra, Y. Shoukry, N. Karamchandani, S. N. Diggavi, and P. Tabuada, "Secure state estimation against sensor attacks in the presence of noise," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 49–59, Mar. 2017.

[10] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2009, pp. 911–918.

[11] L. Guo and J. Ye, "Cyber-physical security of electric vehicles with four motor drives," *IEEE Trans. Power Electron.*, vol. 36, no. 4, pp. 4463–4477, Apr. 2021.

[12] S. Zhuo, A. Gaillard, L. Xu, C. Liu, D. Paire, and F. Gao, "An observer-based switch open-circuit fault diagnosis of DC–DC converter for fuel cell application," *IEEE Trans. Ind. Appl.*, vol. 56, no. 3, pp. 3159–3167, May 2020.

[13] W. Hwang and K. Huh, "Fault detection and estimation for electromechanical brake systems using parity space approach," *J. Dyn. Syst., Meas., Control*, vol. 137, no. 1, Jan. 2015, Art. no. 014504.

[14] D. Xie and X. Ge, "A state estimator-based approach for open-circuit fault diagnosis in single-phase cascaded H-bridge rectifiers," *IEEE Trans. Ind. Appl.*, vol. 55, no. 2, pp. 1608–1618, Mar. 2019.

[15] B. Yang et al., "Enhanced cyber-attack detection in intelligent motor drives: A transfer learning approach with convolutional neural networks," *IEEE J. Emerg. Sel. Topics Ind. Electron.*, vol. 5, no. 2, pp. 710–719, Apr. 2024.

[16] 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 (ITEC)*, Jun. 2022, pp. 991–996.

[17] S. U. Jan, Y.-D. Lee, J. Shin, and I. Koo, "Sensor fault classification based on support vector machine and statistical time-domain features," *IEEE Access*, vol. 5, pp. 8682–8690, 2017.

[18] A. Arsalan et al., "Cyber attack detection and classification for integrated on-board electric vehicle chargers subject to stochastic charging coordination," *Transp. Res. Proc.*, vol. 70, pp. 44–51, Jan. 2023.

[19] B. Yang, J. Ye, and L. Guo, "Fast detection for cyber threats in electric vehicle traction motor drives," *IEEE Trans. Transport. Electrific.*, vol. 8, no. 1, pp. 767–777, Mar. 2022.

[20] L. Guo, J. Ye, and B. Yang, "Cyberattack detection for electric vehicles using physics-guided machine learning," *IEEE Trans. Transport. Electrific.*, vol. 7, no. 3, pp. 2010–2022, May 2020.

[21] M. J. Zideh, P. Chatterjee, and A. K. Srivastava, "Physics-informed machine learning for data anomaly detection, classification, localization, and mitigation: A review, challenges, and path forward," *IEEE Access*, vol. 12, pp. 4597–4617, 2024.

[22] L. Wen, X. Li, L. Gao, and Y. Zhang, "A new convolutional neural network-based data-driven fault diagnosis method," *IEEE Trans. Ind. Electron.*, vol. 65, no. 7, pp. 5990–5998, Jul. 2017.

[23] S.-H. Kim, D.-Y. Yoo, S.-W. An, Y.-S. Park, J.-W. Lee, and K.-B. Lee, "Fault detection method using a convolution neural network for hybrid active neutral-point clamped inverters," *IEEE Access*, vol. 8, pp. 140632–140642, 2020.

[24] B. Gou, Y. Xu, Y. Xia, Q. Deng, and X. Ge, "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. 13281–13294, Dec. 2020.

[25] B. Cai, Y. Zhao, H. Liu, and M. Xie, "A data-driven fault diagnosis methodology in three-phase inverters for PMSM drive systems," *IEEE Trans. Power Electron.*, vol. 32, no. 7, pp. 5590–5600, Jul. 2017.

[26] T. Wang, H. Xu, J. Han, E. Elbouchikhi, and M. E. H. Benbouzid, "Cascaded H-bridge multilevel inverter system fault diagnosis using a PCA and multiclass relevance vector machine approach," *IEEE Trans. Power Electron.*, vol. 30, no. 12, pp. 7006–7018, Dec. 2015.

[27] S. Ye, J. Jiang, J. Li, Y. Liu, Z. Zhou, and C. Liu, "Fault diagnosis and tolerance control of five-level nested NPP converter using wavelet packet and LSTM," *IEEE Trans. Power Electron.*, vol. 35, no. 2, pp. 1907–1921, Feb. 2020.

[28] Z. Y. Xue, K. S. Xiahou, M. S. Li, T. Y. Ji, and Q. H. Wu, "Diagnosis of multiple open-circuit switch faults based on long short-term memory network for DFIG-based wind turbine systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 8, no. 3, pp. 2600–2610, Sep. 2020.

[29] Y. Xia, Y. Xu, and B. Gou, "A data-driven method for IGBT open-circuit fault diagnosis based on hybrid ensemble learning and sliding-window classification," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5223–5233, Aug. 2020.

[30] V. S. B. Kurukuru, M. A. Khan, and S. Sahoo, "Cybersecurity in power electronics using minimal data—A physics-informed spline learning approach," *IEEE Trans. Power Electron.*, vol. 37, no. 11, pp. 12938–12943, Nov. 2022.

[31] J. Zhang, L. Guo, and J. Ye, "Cyber-attack detection for photovoltaic farms based on power-electronics-enabled harmonic state space modeling," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3929–3942, Sep. 2022.

[32] J. Zhang and J. Ye, "Cyber-attack detection for active neutral point clamped (ANPC) photovoltaic (PV) converter using Kalman filter," in *Proc. IEEE Appl. Power Electron. Conf. Exposit. (APEC)*, Mar. 2022, pp. 1939–1944.

[33] J. Zhang et al., "Machine learning-based cyber-attack detection in photovoltaic farms," *IEEE Open J. Power Electron.*, vol. 4, pp. 658–673, 2023.

[34] L. L. Guo, K. Wang, and T. Wang, "Open-circuit fault diagnosis of three-phase permanent magnet machine utilizing normalized flux-producing current," *IEEE Trans. Ind. Electron.*, vol. 71, no. 4, pp. 3351–3360, Apr. 2024.

[35] J. Hang, X. Shu, S. Ding, and Y. Huang, "Robust open-circuit fault diagnosis for PMSM drives using wavelet convolutional neural network with small samples of normalized current vector trajectory graph," *IEEE Trans. Ind. Electron.*, vol. 70, no. 8, pp. 7653–7663, Aug. 2023.

[36] W. Huang et al., "Current-based open-circuit fault diagnosis for PMSM drives with model predictive control," *IEEE Trans. Power Electron.*, vol. 36, no. 9, pp. 10695–10704, Sep. 2021.

[37] F. Wu, Y. Hao, J. Zhao, and Y. Liu, "Current similarity based open-circuit fault diagnosis for induction motor drives with discrete wavelet transform," *Microelectron. Rel.*, vol. 75, pp. 309–316, Aug. 2017.

[38] H. Zhao and L. Cheng, "Open-switch fault-diagnostic method for back-to-back converters of a doubly fed wind power generation system," *IEEE Trans. Power Electron.*, vol. 33, no. 4, pp. 3452–3461, Apr. 2018.

[39] B. Gou, X. Ge, Y. Liu, and X. Feng, "Load-current-based current sensor fault diagnosis and tolerant control scheme for traction inverters," *Electron. Lett.*, vol. 52, no. 20, pp. 1717–1719, Sep. 2016.

[40] G. Ozkan, P. H. Hoang, P. R. Badr, C. S. Edrington, and B. Papari, "Real-time thermal management for two-level active rectifier with finite control set model predictive control," *Int. J. Electr. Power Energy Syst.*, vol. 131, Oct. 2021, Art. no. 107057.

[41] P. R. Badr, G. Ozkan, P. Hoang, C. S. Edrington, and T. Parker, "Multi-objective finite control set model predictive control for interior permanent magnet motors in electric/hybrid-electric vehicles," SAE Tech. Paper, 2022, doi: 10.4271/2022-01-0357.

[42] G. Ozkan, P. Hoang, P. Badr, and C. Edrington, "Electro-thermal control on power electronic converters: A finite control set model predictive control approach," *SAE Int. J. Adv. Current Practices Mobility*, vol. 4, no. 1, pp. 151–156, Apr. 2021.

[43] E. Gumrukcu et al., "Impact of cyber-attacks on EV charging coordination: The case of single point of failure," in *Proc. 4th Global Power, Energy Commun. Conf. (GPECOM)*, Jun. 2022, pp. 506–511.

[44] M. Bozdal, M. Samie, S. Aslam, and I. Jennions, "Evaluation of CAN bus security challenges," *Sensors*, vol. 20, no. 8, p. 2364, Apr. 2020.

[45] H. Kawai, Z. Zhang, R. Kennel, and S. Doki, "Direct speed control based on finite control set model predictive control with voltage smoother," *IEEE Trans. Ind. Electron.*, vol. 70, no. 3, pp. 2363–2372, May 2022.

[46] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, Nov. 1997, doi: 10.1162/neco.1997.9.8.1735.

[47] N. Wagner and J. M. Rondinelli, "Theory-guided machine learning in materials science," *Frontiers Mater.*, vol. 3, p. 28, Jun. 2016.

[48] A. Moradzadeh, B. Mohammadi-Ivatloo, K. Pourhossein, and A. Anvari-Moghaddam, "Data mining applications to fault diagnosis in power electronic systems: A systematic review," *IEEE Trans. Power Electron.*, vol. 37, no. 5, pp. 6026–6050, May 2022.

[49] L. Yang and A. Shami, "On hyperparameter optimization of machine learning algorithms: Theory and practice," *Neurocomputing*, vol. 415, pp. 295–316, Nov. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925231220311693

[50] 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. 13478–13488, Dec. 2021.

[51] S. A. Jawdeh, S. Choi, and C.-H. Liu, "Model-based deep learning for cyber-attack detection in electric drive systems," in *Proc. IEEE Appl. Power Electron. Conf. Expo. (APEC)*, Mar. 2022, pp. 567–573.

[52] M. N. Halgamuge, M. Zukerman, K. Ramamohanarao, and H. L. Vu, "An estimation of sensor energy consumption," *Progr. Electromagn. Res. B*, vol. 12, pp. 259–295, Jan. 2009.

Ali Arsalan (Graduate Student Member, IEEE) received the master's degree in electrical engineering from the University of Engineering and Technology at Lahore, Lahore, Pakistan, in 2019. He is currently pursuing the Ph.D. degree with the Department of Automotive Engineering, International Center for Automotive Research (ICAR), Clemson University, Clemson, SC, USA.

He was a part of the Khwaja Fareed University of Engineering and Information Technology (KFUEIT), Rahim Yar Khan, Pakistan, as a Lab Engineer, for more than five years from 2017 to 2022. He is working as a Graduate Research Assistant at the Secure Energy and Automation Laboratory (SEAL), ICAR, and the Real-Time COntrol and Optimization Laboratory (RT-COOL), Department of Electrical and Computer Engineering (ECE), Clemson University. His research interests include automotive cybersecurity, machine learning, power electronics, electric drive systems, optimization, microgrids, and energy management.

Behnaz Papari (Senior Member, IEEE) received the B.S. degree in electrical engineering from the University of Bushehr, Bushehr, Iran, in 2008, the M.Sc. degree in electrical engineering from the K. N. Toosi University of Technology, Tehran, Iran, in 2011, and the Ph.D. degree in electrical and computer engineering from Florida State University, Tallahassee, FL, USA, in 2018.

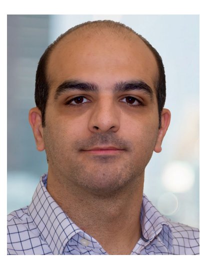
Prior to joining the Department of Automotive Engineering and Electrical and Computer Engineering, Clemson University, Clemson, SC, USA, in Spring 2022, she was an Assistant Professor with the Department of Marine Engineering Technology, Texas A&M University, College Station, TX, USA, and an Assistant Professor of practice with the Energy Production and Infrastructure Center (EPIC), University of North Carolina at Charlotte, Charlotte, NC, USA, for three years, where she taught at undergraduate and graduate levels. Her background is in power systems controls, with an emphasis on modeling, analysis, planning, and artificial intelligence (AI)-based optimization. Her current research interests include distributed controls and secure control frameworks under uncertainty, applications on energy system modeling, stochastic optimization, and electric vehicles, including electric and hybrid-electric and energy storage systems (ESS).

Laxman Timilsina (Member, IEEE) received the B.E. degree in electrical engineering from the Institute of Engineering, Tribhuvan University, Kathmandu, Nepal, in 2016, the M.Sc. degree in distributed generation in electrical engineering from the Institute of Engineering, Kathmandu, Nepal, in 2019, and the Ph.D. degree in electrical engineering from Clemson University, Clemson, SC, USA, in May 2024, under the mentorship of Dr. Christopher S. Edrington.

He was a Graduate Research Assistant with the Real-Time COntrol and Optimization Laboratory (RT-COOL), Holcombe Department of Electrical and Computer Engineering (ECE), Clemson University, where he is currently a Post-Doctoral Researcher Fellow. His research interests include electrified vehicles, integration of renewable energy, ship power systems, and smart grids.

Grace Muriithi (Graduate Student Member, IEEE) received the B.Sc. degree in electrical engineering from the Jomo Kenyatta University of Agriculture and Technology, Juja, Kenya, in 2018, and the M.Sc. degree in electrical engineering from the University of Cape Town, Cape Town, South Africa, in 2022. She is currently pursuing the Ph.D. degree in automotive engineering with the International Centre for Automotive Research, Clemson University, with a focus on enhancing the resilience and security of cyber–physical systems.

Her work contributes to the critical field of automotive cybersecurity in an increasingly electrified and connected transportation landscape. Her research interests encompass cyber–physical systems security, machine learning, energy management, power systems, and vulnerability analysis in advanced control systems. Her research focuses particularly on hybrid electric vehicles (HEVs) and electric vehicle charging stations (EVCSs).



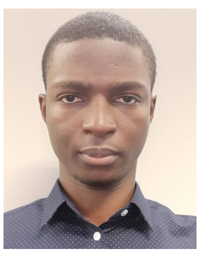
Ali Moghassemi (Graduate Student Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Islamic Azad University, South Tehran Branch, Tehran, Iran, in 2012 and 2015, respectively. He is currently pursuing the Ph.D. degree with Clemson University, Clemson, SC, USA.

He has authored and co-authored several peer-reviewed papers in journals and conferences, two book chapters, and one book. His research interests embrace modeling, simulation, and control of renewable energy systems, partially shaded photovoltaics, power electronics, z-source inverters, power quality, dynamic voltage restorer, and voltage disturbances. His areas of interest include renewable energy systems, power electronics, and power quality.

Mr. Moghassemi has been serving as a reviewer for several scientific journals over the years.

S. M. Imrat Rahman (Graduate Student Member, IEEE) received the B.Sc. degree in electrical and electronic engineering from the Islamic University of Technology, Dhaka, Bangladesh, in 2010, and the M.Sc. degree in power engineering from the Technical University of Munich, Munich, Germany, in 2015. He is currently pursuing the Ph.D. degree with the Holcombe Department of Electrical and Computer Engineering (ECE), Clemson University, Clemson, SC, USA, under the supervision of Dr. Christopher S. Edrington and Dr. Gokhan Ozkan.

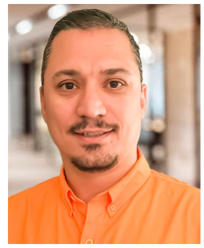
After his M.Sc. degree, he worked as a Lecturer at American International University Bangladesh, Dhaka. He is currently working as a Graduate Research Assistant at the Real-Time COntrol and Optimization Laboratory (RT-COOL). His research areas include active thermal management of power electronic converters, distributed control, and thermal modeling of power electronic building block (PEBB) systems.



Elutunji Buraimoh (Graduate Student Member, IEEE) received the B.Tech. degree (Hons.) in electronic and electrical engineering from the Ladoke Akintola University of Technology, Ogbomoso, Nigeria, in 2012, the M.Sc. degree in electronic and electrical engineering from Obafemi Awolowo University, lfe, Nigeria, in 2016, and the D.Eng. degree from Durban University of Technology, Durban, South Africa, in 2021. He is currently pursuing the Ph.D. degree in electrical engineering with Clemson University, Clemson, SC, USA.

His current research focus is the geographically distributed real-time co-simulation of power systems, communication latency compensation, and energy management. His previous studies focused on microgrids, renewable energy, power systems control, and flexible alternating current transmission (FACTS) devices.

Mr. Buraimoh is a Registered Engineer of Council for the Regulation of Engineering in Nigeria (COREN), a Corporate Member of Nigeria Society of Engineers (NSE), a member of Society of Automotive Engineers (SAE), and a candidate for Engineering Council of South Africa (ECSA).



Gokhan Ozkan (Senior Member, IEEE) received the B.Sc. degree from the Electrical Education Department, Marmara University, Istanbul, Turkey, in 2006, the B.Sc. (as a Valedictorian) and M.Sc. degrees from the Energy System Engineering Department, Erciyes University, Kayseri, Türkiye, in 2014 and 2016, respectively, and the Ph.D. degree from the Electrical and Computer Engineering Department, Florida State University, Tallahassee, FL, USA, in 2019.

In 2020, he joined Clemson University, Clemson, SC, USA, as a Post-Doctoral Fellow, where he has been a Research Assistant Professor with the Holcombe Department of Electrical and Computer Engineering since 2021. He is currently a Research Lead with the Energy Innovation Center, North Charleston, SC, USA, and the Manager of the Real-Time COntrol and Optimization Laboratory (RT-COOL), Clemson University. His main research interests include power systems and distributed energy resources (DER) integration; model predictive control in power converters and drives; active thermal management and fault-tolerant control; distributed controls; power and electromagnetic (EM); and real-time power distribution system modeling, simulation, co-simulations, and hardware-in-the-loop instantiation.

Christopher S. Edrington (Senior Member, IEEE) received the B.S. degree in engineering from Arkansas State University, Jonesboro, AR, USA, in 1999, and the M.S. and Ph.D. degrees in electrical engineering from Missouri University of Science and Technology, Rolla, MO, USA, in 2001 and 2004, respectively.

He was a GAANN and IGERT Fellow of Missouri University of Science and Technology. From 2004 to 2007, he was an Assistant Professor in electrical engineering with the College of Engineering, Arkansas State University. From 2007 to 2019, he held the ranks of an Assistant Professor, an Associate Professor, and a Full Professor in electrical and computer engineering with the FAMU-FSU College of Engineering and was the Lead of the Energy Conversion and Integration Thrust, Center for Advanced Power Systems, Florida State University, Tallahassee, FL, USA. In 2019, he joined Clemson University, Clemson, SC, USA, as the Warren H. Owen Distinguished Professor of Electrical and Computer Engineering, where he leads the Real-Time COntrol and Optimization Laboratory (RT-COOL). He is currently an Associate Director of Industry Relations, VIPR-GS Center, Clemson University. His research interests include modeling, simulation, optimization, and control of electromechanical drive systems; applied power electronics; and integration of renewable energy, storage, pulse power loads, and hardware-in-the-loop (HIL) VV&A experimentation.