A Four-layer Cyber-physical Security Model for Electric Machine Drives considering Control Information Flow

Bowen Yang, *Student Member, IEEE,* He Yang, *Student Member, IEEE,* Jin Ye, *Senior Member, IEEE*

***Abstract*—Despite the IEEE Power Electronics Society (PELS) establishing Technical Committee 10 on Design Methodologies with a focus on the cyber-physical security of power electronics systems, a holistic design methodology for addressing security vulnerabilities remains underdeveloped. This gap largely stems from the limited integration of computer science and power/control engineering studies in this interdisciplinary field. Addressing the inadequacy of unilateral cyber or control perspectives, this paper presents a novel four-layer cyber-physical security model specifically designed for electric machine drives. Central to this model is the innovative Control Information Flow (CIF) model, residing within the control layer, which serves as a pivotal link between the cyber layer's vulnerable resources and the physical layer's state-space models. By mapping vulnerable resources to control variable space and tracing attack propagation, the CIF model facilitates accurate impact predictions based on tainted control laws. The effectiveness and validity of this proposed model are demonstrated through hardware experiments involving two typical cyber-attack scenarios, underscoring its potential as a comprehensive framework for multidisciplinary security strategies.**

***Index Terms*—electric machine drives, cyber security, impact analysis, cyber-physical systems.**

ABBREVIATIONS

PELS	Power Electronics Society
CIF	Control Information Flow
SCADA	Supervisory Control and Data Acquisition
SRAM	Static Random-access Memory
MCU	Microcontroller
DSP	Digital Signal Processors
CAN	Controller Area Networks
ADC	Analog-to-digital Converter
PI	Proportional-integral
FOC	Field-oriented Control
PMSM	Permanent Magnet Synchronous Motor
ISR	Interrupt Service Routine
PWM	Pulse-width Modulation
DQZ	Direct Quadrature Zero
FDI	False Data Injection

I. INTRODUCTION

The IEEE Power Electronics Society (PELS) has established Technical Committee 10 on Design Methodologies, tasked with the development of hardware and software tools for power electronics design, with a particular focus on ensuring the data communication and cyber-physical security of power electronics systems. In recent times, there has been a growing concern for the security and safety of modern electric machine drives due to the increasing adoption of digital control and networking. In particular, with the fast expansion of electric vehicles, wind power generation, and intelligent manufacturing systems, the number of digitally-controlled electric machine drives is growing dramatically. Therefore, electric machine drives present attractive targets for cyber-physical attacks due to their critical operational roles. A significant vulnerability arises from the interplay between rapid advancements in network and communication technologies and the increasing automation and intelligence of systems. Communication networks commonly employed in these drives, including CAN bus for electric vehicles and ModBus for manufacturing systems, often lack sufficient cyber-security measures. Furthermore, the embedded controllers in these drives are generally constrained by limited computational resources. Coupled with the trend towards higher switching frequencies in power electronics, the firmware often does not include adequate onboard detection or countermeasures against cyber threats. This nexus of high-value assets and inadequate protections renders them particularly susceptible to cyber-attacks, as evidenced by notable incidents like the Stuxnet attacks in 2010 [1], the Jeep Cherokee Hack in 2015 [2], the Ukrainian power grid attack in 2015 [3], and the Tesla T BONE attacks in 2020 [4].

Existing security literature on power and industrial systems, however, primarily focuses on the system level like supervisory control and data acquisition (SCADA) systems [5], [6], micro-grids [7], and industrial control systems [8]. A secure control model proposed in [9] and a physics-based detection model in [10] represent primary approaches to analyze and detect cyber-attacks in electric machine drives [11], [12]. Additionally, computer scientists have focused their cyber security research on vulnerabilities of industrial controllers and their communication protocols, such as SRAMs of microcontrollers (MCU) / digital signal processors (DSP) [13], controller area networks (CAN) [14], [15], and Modbus protocols [16]. To our knowledge, security vulnerability of electric machine drives have not yet been studied comprehensively[11], [17], [18]. A comprehensive design methodology for studying the security vulnerabilities of these systems has been lacking, primarily due to a gap in vulnerability studies conducted by computer

This research was partially supported by U.S. National Science Foundation ECCS-EPCN 2102032 and NSF-SATC-2019311, and U.S. Department of the Air Force FA8571-20-C-0017.

B. Yang, H. Yang and J. Ye are with Intelligent Power Electronics and Electric Machine Laboratory, University of Georgia, Athens, GA 30602, USA (e-mail: bowen.yang@uga.edu, he.yang@uga.edu, jin.ye@uga.edu).

scientists and power/control engineers in this interdisciplinary field. This gap will be summarized as follows:

1) Computer scientists have identified vulnerabilities in specific devices and protocols, including MCU, DSP, CAN, and Modbus[13]–[16], [19]. However, they have not established a clear connection between these vulnerabilities and their potential impact on physical infrastructure, such as inverters for electric machine drives.
2) Engineers frequently employ state-space models and transfer function-based models for controlling systems, as noted in various studies [9], [10], [17]. These models often presuppose that cyber-attack strategies directly affect control commands $\mathbf{u}$ and system feedback $\mathbf{y}$, as depicted in Fig. 1. However, a significant challenge arises in correlating $\mathbf{u}$ and $\mathbf{y}$ with actual vulnerable resources identified in computer science research. This disconnect hinders accurate predictions of the real-world impact of cyber-attacks on physical systems, necessitating more integrated and realistic modeling approaches.

TABLE I
SUMMARY OF LITERATURE FROM CYBER- AND PHYSICAL-DOMAINS

Domain	Focuses & Literature
Cyber	Research[13]–[16] delves into the vulnerabilities of firmware and communication protocols, highlighting a progression from hardware faults to advanced network security threats, emphasizing the need for robust countermeasures.
Cyber-Physical	Research [5], [6], [9]–[12], [17] focus on enhancing the security and resilience of SCADA systems and electric vehicle systems, evolving from general intrusion detection to specific challenges in attack-resilient system design.
This Paper's Focus	Presents a new four-layer cyber-physical security model, centered around the CIF model, for electric machine drives ,offering a comprehensive framework to predict and counteract cyber-attacks effectively.

Due to these two reasons, there is a disconnect between computer science and power/control engineering research, and it's challenging to connect real-world cyber threats to specific physical systems. This gap poses a significant obstacle to ensuring security and safety in modern electric machine drives with widespread use of digital control units. To address this gap, this paper introduces a novel four-layer cyber-physical security model tailored for electric machine drives, including cyber layer, control layer, physical layer, and impact layer. Fig. 1 shows a conceptual diagram for the proposed model and compares with the traditional model. The proposed model initially converts vulnerable resources, such as firmware and protocols, into equivalent 'tainted' sources using the attack adversary resource model. These unified tainted sources are subsequently mapped onto the control-information-flow (CIF) model. Within the CIF model, all control-related resources are organized according to the implemented control laws, tracing the tainted sources through the controller's information flow. This process results in a set of tainted control laws. The physical layer then integrates these tainted control laws with the physical plant's dynamics. Finally, the impact layer calculates the system dynamics under cyber-attacks, extracting the resulting impacts and potential attack patterns and characteristics. By employing a novel CIF model in the control layer, this proposed model forges a link between cyber-domain analysis and physical plant dynamics, offering valuable insights into various cyber-attack scenarios and enabling accurate predictions of impacts and attack pattern abstraction. At the heart of this proposed model lies an innovative Control Information Flow (CIF) model within the control layer, originated from the classic information flow model [20], [21] and taint graph analysis [22] from informatics research. This CIF model effectively identifies vulnerable resources within the control variable space and traces the paths through which attacks on control variables propagate to affect control laws. Subsequently, accurate predictions of the impact of these attacks can be made by solving the system's state-space model associated with the tainted control laws.

This paper's contributions can be summarized as follows:

1) Introduction of a novel four-layer cyber-physical security model designed specifically for electric machine drives. Notably, it stands as one of the pioneering models aimed at closing the gap between the power/control engineering and computer science communities.
2) Introduction of the CIF model, which plays a pivotal role in bridging the divide between vulnerable resources within the cyber layer and the state-space models found in the physical layer.
3) Facilitation of precise impact predictions for cyber-attacks by solving the system's state-space model associated with tainted control laws.

The rest of the paper is organized as follows. Section II will describe the proposed security model. Section III will provide two case studies demonstrating the proposed model. Section IV will provide experiment results for validations, and section V will address the conclusion.

II. SECURITY MODEL FOR DIGITALLY-CONTROLLED ELECTRIC MACHINE DRIVES

The proposed model consists of four layers: cyber layer, control layer, physical layer, and impact layer. Fig. 1 shows a diagram of the proposed four-layer security model for electric machine drives. The cyber layer formulates the vulnerable resources and potential cyber-attacks into a list of tainted sources (α). The control layer tracks the propagation of these tainted sources and generates the tainted control laws (α_u, α_y, $\hat{\mathbf{g}}$, $\hat{\mathbf{h}}$). The physical layer maps the tainted control laws to the original system dynamics and calculates the state trajectories under the attack. Finally, the impact layer defines two metrics evaluating attack impacts based on the predicted state trajectories. Importantly, attacks on power electronics controllers typically target controller firmware, distinguishing them from command-based attacks that exploit vulnerabilities in software applications, operating systems, or networks. While a variety of attacks can target controller firmware, their ultimate impact on power electronics systems is primarily mediated through the interface between the controller and power converters, especially the Pulse Width Modulation (PWM) modulation commands. Our model is designed to trace various cyber-attacks from their origins to the PWM interfaces, starting by identifying potential taint sources in the cyber layer, such as

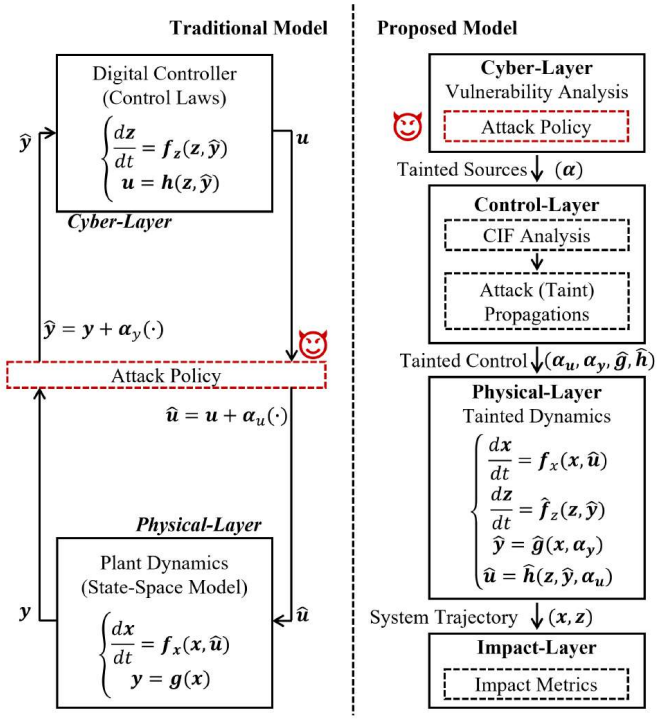


Fig. 1. Comparison between the traditional impact analysis model (left) and the proposed security model (right).

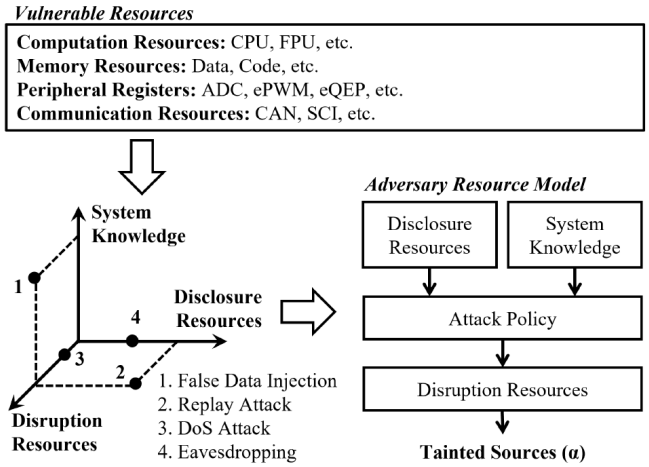


Fig. 2. Diagram of the cyber layer based on the adversary resource model.

malicious control commands or compromised firmware. These sources are then mapped onto a Control Information Flow (CIF) model, tracing their propagation to the PWM interface and facilitating the generation of potential attack impacts, including disturbance patterns and characteristic frequencies vital for the development of future detection algorithms. Nonetheless, the primary focus of this paper is on analyzing the impact of such attacks.

A. Cyber Layer

Existing literature has explored vulnerable resources in MCUs and DSPs, such as SRAMs [13], CAN [14], [15], and Modbus protocols [16]. These vulnerable resources suffer from various cyber-attacks, such as buffer overflows, man-in-the-middle attacks, and false data injections (FDI). Although most power electronics devices inherently lack networking capabilities, they often function as subsystems within larger industrial applications. These include electric machine drives in manufacturing systems and power inverters in modern power grids. While these target devices might not be directly connected to networks, they frequently communicate with higher-level controllers or communication management systems. Consequently, compromising these devices is feasible, as demonstrated by the TBONE attacks targeting Tesla motor drives during the Pwn2Own 2020 event [4]. Moreover, standalone or physically isolated systems are not impervious to threats, remaining vulnerable to insider or physical attacks. Notable incidents at major corporations like Tesla, Microsoft, Yahoo, and Google [23], as well as supply chain attacks at Applied Materials [24], underscore these vulnerabilities. Our proposed model aims to evaluate the impacts of such attacks during the design and development stages, offering critical insights into mitigating potential risks. Furthermore, it is important to clarify that the cyber layer within our proposed framework is not intended for intrusion detection. Instead, its primary function is to transform identified intrusions and vulnerabilities, as determined by various analyses in the cyber domain, into equivalent tainted sources. These sources are subsequently integrated into the Control-Information-Flow (CIF) model within the control layer. This process emphasizes the role of the cyber layer as a translator between identified cyber threats and their potential impacts on the control dynamics of the system. The cyber layer adopts the adversary resource model to formulate these attacks to a list of tainted sources in the controller (α). Fig. 2 shows a diagram of the cyber layer, which first categorizes vulnerable resources into system knowledge, disclosure resources, and disruption resources. The system knowledge includes critical information about the controllers, such as variable locations, control-law-related function instances, and communication protocols. The disclosure and disruption resources are defined by the attacker's access permissions of specific onboard resources. Then, the adversary resource model connects the system knowledge and disclosure resources to the disruption resources using a formulated attack policy and generates a list of tainted sources. Such tainted sources will then be mapped to the CIF model in the control layer as the starting point of the attack propagation analysis. To illustrate the process of converting a cyber-attack into a tainted source within the CIF model, the following example demonstrates a simplified buffer-overflow attack. This example is specifically chosen to exemplify how typical vulnerabilities can be mapped and analyzed within our framework. Suppose the address for the inverter phase A current ADC offset variable (x_{A0}) is 0x00C000 - 0X00C001 (the data type for the offset variable is int32), and there is a vulnerability report stating that there is a potential threat of buffer-overflows at 0x00C000 - 0x00CFFF. The cyber layer will first determine that x_{A0} is the only variable stored in 0x00C000 - 0x00CFFF and map x_{A0} to the CIF model as a tainted source. Meanwhile, the tainted x_{A0} will be denoted

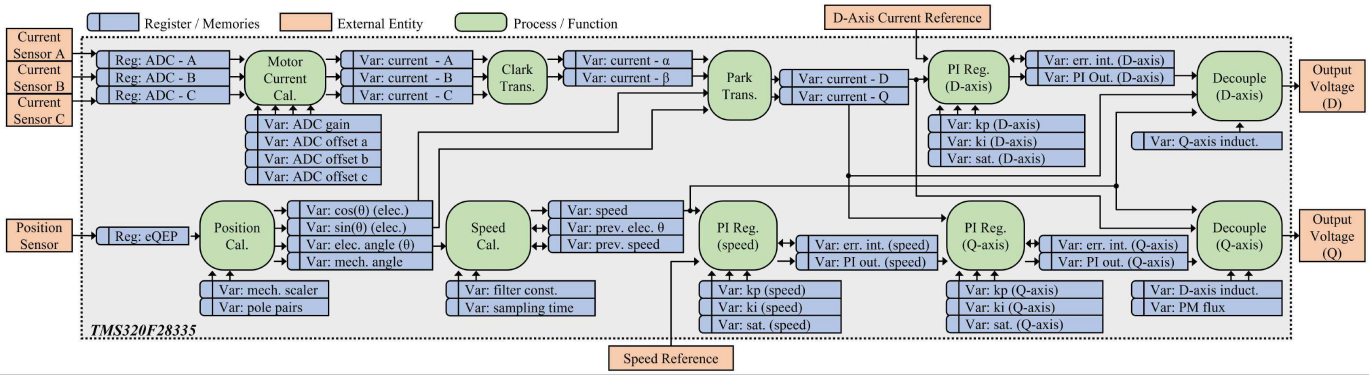


Fig. 3. Diagram of the control information flow (CIF) model for a PMSM drive with field-oriented-control (FOC).

as $\hat{x}_{A0} = x_{A0} + \alpha$, since x_{A0} could be falsely modified by buffer-overflows. Then, the propagation and impacts of this threat will be analyzed in the control layer.

B. Control Layer

The proposed security model centers around the control layer, which is built on an innovative CIF model capable of identifying and developing control strategies for tainted sources from the cyber layer, which link between physical layer and cyber threats.

In the realm of cyber-physical security for control systems, prior research typically relied on a model presented in [9]. Fig. 1 provides a comparison between the conventional analysis model and the proposed security model when assessing the impact of attacks on electric machine drives. The traditional control model assumes that attack policies are directly integrated into feedback signals $\mathbf{y}$ and control outputs $\mathbf{u}$. In Fig. 1, a common attack model is illustrated, where α_y and α_u represent predefined functions based on attack policies. However, real-world cyber-attacks involve intricate interactions among various resources and processes, rendering the traditional model insufficient for capturing and analyzing these interactions, as well as the propagation and impact of attacks.

As shown in Fig. 1, the control layer adopts a proposed control information flow (CIF) model, to fill the gap between real-world attacks and control system analysis. The CIF model categorizes different onboard resources into processes/functions, registers/memories, and external entities.

1) Processes/Functions: Recent developments in control firmware tend to be modularized, which means control functions are packed into flexible modules. These modules range from ADC data conversions to proportional-integral(PI) controllers. As these modules determine the overall structures of the digital controller, they will be the backbone of the CIF model and be constructed first.

2) Registers/Memories: There are three associated data types for each process/function: inputs, outputs, and parameters. These data represent the information flowing in and out of each process/function and are stored in registers and memories (data sector). In the CIF model, inputs, outputs, and parameters are defined as registers/memories block with different locations with respect to their processes/functions.

3) External Entities: Besides processes/functions and registers/memories, various peripheral units are associated with digital controllers' interactions with external information, such as sensor signals.

For example, Fig. 3 shows the CIF model based on the field-oriented-control (FOC) for a permanent magnet synchronous machine (PMSM). The three types of resources are denoted as processes/functions (green blocks), registers/memories (blue blocks), and external entities (orange blocks). In DSP/MCU-controlled electric machine drive systems, the interrupt service routine (ISR) is the primary manner to implement the control algorithms. Therefore, their execution sequences determine the arrangement of processes/functions. Then, inputs, outputs, and pre-defined parameters are aligned with each process/function. If a process/function reads and writes to the same variable in one control cycle, this variable is set on the right of this process/function. In the end, the peripheral units are located outside processes/functions and registers/memories.

The CIF model adapts to various cyber threats. For control logic vulnerabilities, PWM modulations can be simplified to voltage outputs(Fig. 3). For attacks on speed calculations, add details like digital low-pass filters using extra registers/memories blocks. This flexibility makes CIF adaptable to diverse vulnerabilities.

After establishing the CIF model, the control layer identifies tainted sources (α) in the cyber layer. The propagation of these sources is tracked through paths (Fig. 4 and Fig. 5) Once the propagation paths are determined, tainted control laws (α_u, α_y, $\hat{\mathbf{g}}$, $\hat{\mathbf{h}}$) are extracted and sent to the physical layer.

C. Physical Layer

The physical layer consists of the state-space model of the electric machine drive. For example, the dynamics of a PMSM drive in DQZ reference frame could be modeled as Eq. (1)-Eq. (3), where ω_m, i_d, i_q are the speed, d-axis current, and q-axis current; J, R_m, T_L are the inertia, damping coefficient, and load torque; R_s, L_s, λ_{PM} are the stator resistance,

inductance, and magnet flux linkage.

$$\frac{d\omega_m}{dt} = -\frac{R_m}{J}\omega_m + \frac{\lambda_{PM}}{J}i_q - \frac{T_L}{J} \tag{1}$$

$$\frac{di_d}{dt} = (-\frac{R_s}{L_s}i_d + \omega_m i_q + \frac{1}{L_s}v_d)\cdot\omega_b \tag{2}$$

$$\frac{di_q}{dt} = (-\frac{R_s}{L_s}i_q - \omega_m i_d - \omega_m\frac{\lambda_{PM}}{L_s} + \frac{1}{L_s}v_q)\cdot\omega_b \tag{3}$$

v_d and v_q are the d- and q-axis voltage inputs, which are derived from the FOC laws shown in Eq. (4)-Eq. (11), where I_d, I_q, Ω_m are the references of d-axis current, q-axis current and motor speed; z_d, z_q, z_m are the error integration from PI regulators; K_{mp}, K_{mi}, K_{dp}, K_{di}, K_{qp}, K_{qi} are the PI control coefficients. All variables in Eq. (1)-Eq. (11) are in per-unit manner where ω_b is the base value for synchronous speed.

$$\frac{dz_m}{dt} = \Omega_m - \omega_m \tag{4}$$

$$\frac{dz_d}{dt} = I_d - i_d \tag{5}$$

$$\frac{dz_q}{dt} = I_q - i_q \tag{6}$$

$$I_q = K_{mp}(\Omega_m - \omega_m) + K_{mi}\cdot z_m \tag{7}$$

$$u_d = K_{dp}(I_d - i_d) - K_{di}\cdot z_d \tag{8}$$

$$u_q = K_{qp}(I_q - i_q) + K_{qi}\cdot z_q \tag{9}$$

$$v_d = u_d - \omega_m L_s i_q \tag{10}$$

$$v_q = u_q + \omega_m L_s i_d + \omega_m\lambda_{PM} \tag{11}$$

Then, the physical layer will replace the original control laws, i.e., Eq. (4)-Eq. (11), with the tainted control laws from the control layer and solve the close-loop system to get the system state trajectories under specific attacks.

D. Impact Layer

After obtaining system state trajectories with specific attacks, assess the attack impact using defined attack properties and system metrics.

Definition 1. *Given a continuous state space $\mathbf{X} \subseteq \mathbb{R}^n$, suppose the original closed-loop attack-free system $\dot{\mathbf{x}} = f(\mathbf{x})$ has an equilibrium point $\mathbf{X_e}$, and there exists a set $\mathbb{B}^n$, which satisfies: (1) $\mathbb{B}^n \subseteq \mathbb{R}^n$; (2) $\mathbf{X_e} \subseteq \mathbb{B}^n$; (3) for any initial point $\mathbf{X_0} \subseteq \mathbb{B}^n$, the state space $\mathbf{X}$ will eventually converge to the equilibrium point $\mathbf{X_e}$. Meanwhile, suppose the tainted closed-loop system $\dot{\mathbf{x}} = \hat{f}(\mathbf{x})$ has a stable equilibrium point $\mathbf{X_a}$ and let T_0 be the attack-initiating time and T be the time when the attack could be detected and removed. Then, the attack is (1) "minor" if $||\mathbf{X_e} - \mathbf{X_a}|| \leq \delta$, δ is a small positive number; (2) "stable" if $||\mathbf{X_e} - \mathbf{X_a}|| > \delta$ and $\mathbf{X_a} \subseteq \mathbb{B}^n$; (3) "drastic" if $\mathbf{X_a} \nsubseteq \mathbb{B}^n$ and $\mathbf{X}(T) \subseteq \mathbb{B}^n$; (4) "unstable" if $\mathbf{X_a} \nsubseteq \mathbb{B}^n$ and $\mathbf{X}(T) \nsubseteq \mathbb{B}^n$.*

Remark 1. *If $\mathbf{X_e}$ is a globally stable equilibrium point, i.e., $\mathbb{B}^n = \mathbb{R}^n$ and $\mathbf{X_a}$ is a stable equilibrium point, all attacks will be "minor" or "stable".*

Remark 2. *If the tainted closed-loop system $\dot{\mathbf{x}} = \hat{f}(\mathbf{x})$ has an unstable equilibrium point $\mathbf{X_a}$, the attack is "unstable".*

Definition 2. *Define the first impact index $\mathcal{I}_1$ as the cost required to steer the system states back to origin, i.e.,*

$$\mathcal{I}_1 = \sqrt{\int_T^\infty ||\mathbf{x}(t) - \mathbf{X_e}||^2 dt} \tag{12}$$

Definition 3. *Define the second impact index $\mathcal{I}_2$ as the maximum system deviation from the original equilibrium point, i.e.,*

$$\mathcal{I}_2 = \max\{||\mathbf{x}(t) - \mathbf{X_e}|| : t \in [T_0, T]\} \tag{13}$$

Remark 3. *If the attack is "unstable", $\mathcal{I}_1$ will not be convergent.*

Based on **Definition 2** and **Definition 3**, the first impact index gauges system recovery difficulty, while the second index measures attack-induced disturbance. The security model outlines a systematic attack impact analysis procedure:

- 1. Cyber Layer:Identify vulnerable resources, create attack policy, and generate tainted sources.
- 2. Control Layer: Map taint sources to CIF model, track attack paths, and establish tainted control laws.
- 3. Physical Layer: Substitute original control laws with tainted ones, solve the tainted closed-loop state-space model, and compute state trajectories during attacks.
- 4. Impact Layer: Assess attack impacts and compute impact metrics.

III. Impact Analysis of Electric Machine Drives Due to Cyber-Attacks: Case Studies

This section presents two case studies demonstrating the impact analysis for cyber-attacks on electric machine drives with the proposed security model. These case studies involve an FDI attack on a motor current sensor offset and another FDI attack on the calculated motor speed feedback.

A. Case 1: FDI attack on the motor current offset variable

This case study focuses on an FDI attack on the motor phase A current sensor offset variable. As per the proposed security model, the tainted variable and attack policy are represented in Eq. (14), with $x_{offsetA}$ and $\hat{x}_{offsetA}$ denoting the original and attacked motor phase A current offset variables, α is the attack coefficient.

$$\hat{x}_{offsetA} = x_{offsetA} + \alpha \tag{14}$$

After mapping Eq. (14) to the CIF model, Fig. 4 shows the attack propagation path. Then tainted control laws could be extracted by substituting Eq. (14) to each process/function along the propagation path.

1) Motor Current Calculation Process:

$$\hat{i_a} = i_a - k_{adc}\cdot\alpha \tag{15}$$

where k_{adc} is the ADC convertion coefficient.

2) Clark Transformation Process:

$$\hat{i}_\alpha = i_\alpha - \frac{2}{3}k_{adc}\cdot\alpha \tag{16}$$

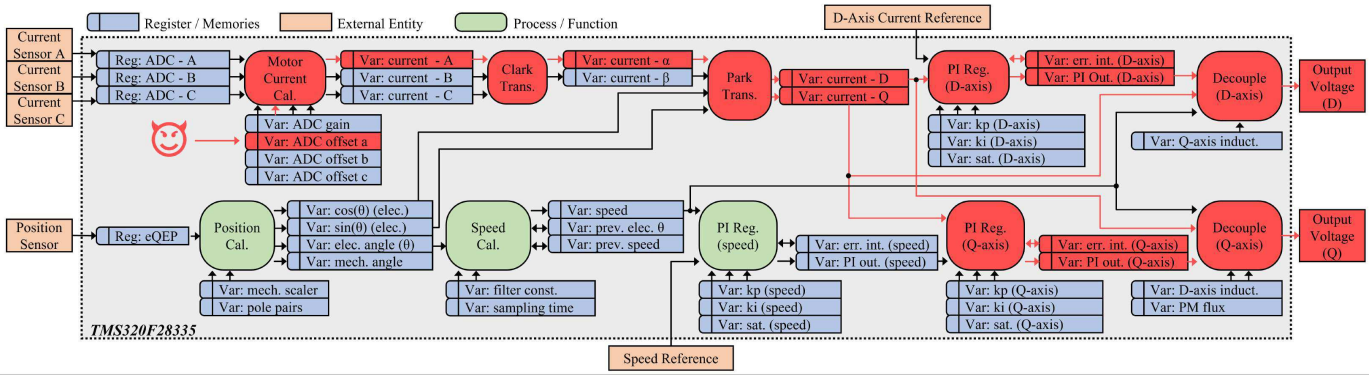


Fig. 4. Diagram of the attack propagation tracing for case 1.

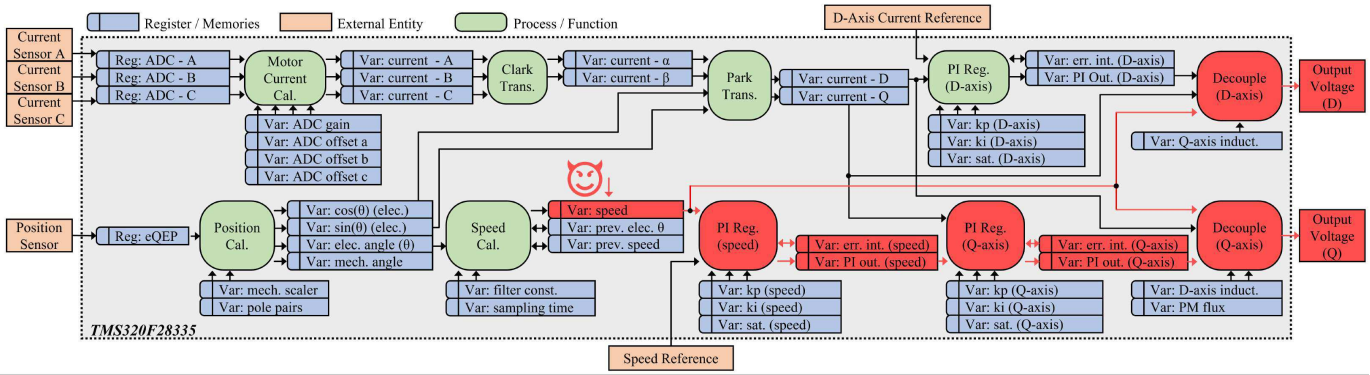


Fig. 5. Diagram of the attack propagation tracing for case 2.

3) Park Transformation Process:

$$\hat{i}_d = i_d - \frac{2}{3}k_{adc} \cdot \cos\theta \cdot \alpha \tag{17}$$

$$\hat{i}_q = i_q + \frac{2}{3}k_{adc} \cdot \sin\theta \cdot \alpha \tag{18}$$

where θ is the electric angle per unit.

4) D-Axis Current PI Regulator Process: As the PI regulator includes the error integral term, the D-axis control state equation is changed as the follow.

$$\frac{d\hat{z}_d}{dt} = I_d - \hat{i}_d = I_d - (i_d - \frac{2}{3}k_{adc}\cos\theta \cdot \alpha) \tag{19}$$

Meanwhile, the PI regulator output will change accordingly.

$$\hat{u}_d = K_{dp}(I_d - (i_d - \frac{2}{3}k_{adc}\cos\theta \cdot \alpha)) - K_{di} \cdot \hat{z}_d \tag{20}$$

5) Q-Axis Current PI Regulator Process:

$$\frac{d\hat{z}_q}{dt} = I_q - \hat{i}_q = I_q - (i_q + \frac{2}{3}k_{adc}\sin\theta \cdot \alpha) \tag{21}$$

$$\hat{u}_q = K_{qp}(I_q - (i_q + \frac{2}{3}k_{adc}\sin\theta \cdot \alpha)) - K_{qi} \cdot \hat{z}_q \tag{22}$$

6) D-Axis and Q-Axis Feedforward Decoupling Process: this process is the final stage of the FOC control and generates the d- and q-axis voltage commands.

$$\hat{v}_d = \hat{u}_d - \omega_m L_s(i_q + \frac{2}{3}k_{adc}\sin\theta \cdot \alpha) \tag{23}$$

$$\hat{v}_q = \hat{u}_q + \omega_m(L_s(i_d - \frac{2}{3}k_{adc}\cos\theta \cdot \alpha) + \lambda_{PM}) \tag{24}$$

Stacking the above results will generate tainted control laws, which are shown in Eq. (25)-Eq. (32).

$$\frac{dz_m}{dt} = \Omega_m - \omega_m \tag{25}$$

$$\frac{d\hat{z}_d}{dt} = I_d - (i_d - \frac{2}{3}k_{adc} \cdot \cos\theta \cdot \alpha) \tag{26}$$

$$\frac{d\hat{z}_q}{dt} = I_q - (i_q + \frac{2}{3}k_{adc} \cdot \sin\theta \cdot \alpha) \tag{27}$$

$$I_q = K_{mp}(\Omega_m - \omega_m) + K_{mi} \cdot z_m \tag{28}$$

$$\hat{u}_d = K_{dp}(I_d - (i_d - \frac{2}{3}k_{adc} \cdot \cos\theta \cdot \alpha)) - K_{di} \cdot \hat{z}_d \tag{29}$$

$$\hat{u}_q = K_{qp}(I_q - (i_q + \frac{2}{3}k_{adc} \cdot \sin\theta \cdot \alpha)) + K_{qi} \cdot \hat{z}_q \tag{30}$$

$$\hat{v}_d = \hat{u}_d - \omega_m L_s(i_q + \frac{2}{3}k_{adc} \cdot \sin\theta \cdot \alpha) \tag{31}$$

$$\hat{v}_q = \hat{u}_q + \omega_m L_s(i_d - \frac{2}{3}k_{adc} \cdot \cos\theta \cdot \alpha) + \omega_m \lambda_{PM} \tag{32}$$

Then, the physical layer will replace Eq. (4)-Eq. (11) with Eq. (25)-Eq. (32) and solves the state trajectories under attacks.

B. Case 2: FDI attack on the motor speed feedback variable

Besides current offset variables, the calculated speed feedback is also a vulnerable target of malicious attacks. For example, the Stuxnet worm compromised the industrial control system by manipulating the rotating speeds of industrial motor drives [25]. Suppose the attack policy is the same as Eq. (14),

TABLE II
SPECIFICATIONS OF THE EXPERIMENT PLATFORM.

Rated Power	1.5 kW	Stator Resistance	0.4050 Ω
Rated Current	8.2 A	Stator Inductance	0.0024 mH
DC Bus Voltage	200 V	Magnet Flux Linkage	0.0599 Wb
Rated Frequency	250 Hz	Number of Pole Pairs	5
Control Frequency	10 kHz	Motor Inertia	3.10e-4 kgm^2

which is shown in Eq. (33), where ω_m and $\hat{\omega}_m$ is the original and attacked motor speed feedback variables.

$$\hat{\omega}_m = \omega_m + \alpha \tag{33}$$

After mapping Eq. (33) to the CIF model, Fig. 5 shows the attack propagation path. Then tainted control laws are derived:

1) Speed PI Regulator Process:

$$\frac{d\hat{z}_m}{dt} = \Omega_m - \hat{\omega}_m = \Omega_m - (\omega_m + \alpha) \tag{34}$$

$$\hat{I}_q = K_{mp}(\Omega_m - (\omega_m + \alpha)) + K_{mi} \cdot \hat{z}_m \tag{35}$$

2) Q-Axis Current PI Regulator Process:

$$\frac{d\hat{z}_q}{dt} = \hat{I}_q - i_q \tag{36}$$

$$\hat{u}_q = K_{qp}(\hat{I}_q - i_q) + K_{qi} \cdot \hat{z}_q \tag{37}$$

3) D-Axis and Q-Axis Feedforward Decoupling Process:

$$\hat{v}_d = u_d - (\omega_m + \alpha)L_s i_q \tag{38}$$

$$\hat{v}_q = \hat{u}_q + (\omega_m + \alpha)L_s i_d + (\omega_m + \alpha)\lambda_{PM} \tag{39}$$

Stacking above results will generate tainted control laws, which are shown in Eq. (40)-Eq. (47).

$$\frac{d\hat{z}_m}{dt} = \Omega_m - \hat{\omega}_m = \Omega_m - (\omega_m + \alpha) \tag{40}$$

$$\frac{dz_d}{dt} = I_d - i_d \tag{41}$$

$$\frac{d\hat{z}_q}{dt} = \hat{I}_q - i_q \tag{42}$$

$$\hat{I}_q = K_{mp}(\Omega_m - (\omega_m + \alpha)) + K_{mi} \cdot \hat{z}_m \tag{43}$$

$$u_d = K_{dp}(I_d - i_d) - K_{di} \cdot z_d \tag{44}$$

$$\hat{u}_q = K_{qp}(\hat{I}_q - i_q) + K_{qi} \cdot \hat{z}_q \tag{45}$$

$$\hat{v}_d = u_d - (\omega_m + \alpha)L_s i_q \tag{46}$$

$$\hat{v}_q = \hat{u}_q + (\omega_m + \alpha)L_s i_d + (\omega_m + \alpha)\lambda_{PM} \tag{47}$$

Then, the physical layer will replace Eq. (4)-Eq. (11) with Eq. (40)-Eq. (47) and solves the state trajectories under attacks.

IV. EXPERIMENT VALIDATIONS

This section will continue with the impact analysis in section III. The physical layer solves the tainted system dynamics and generates system state trajectories under attack. Meanwhile, this section will also provide hardware experiment results to support the analysis results from the proposed model.

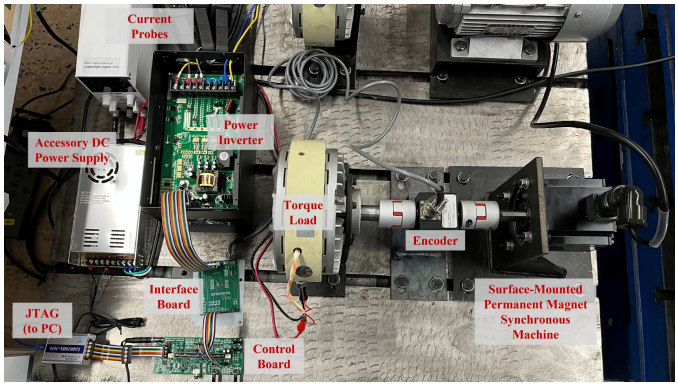


Fig. 6. Picture of the hardware experiment platform with a PMSM drive.

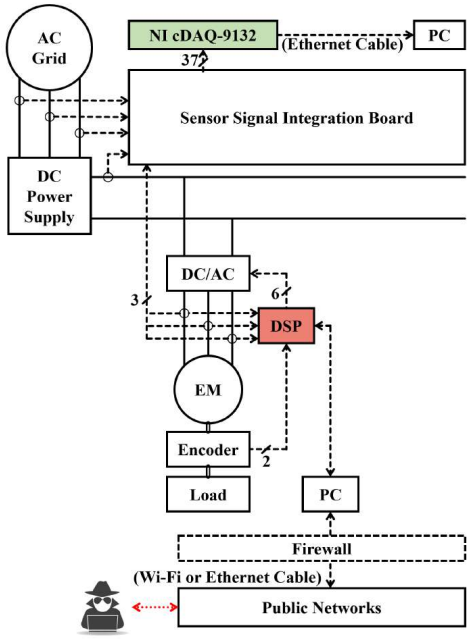


Fig. 7. Concept diagram of the hardware experiment platform with a PMSM drive.

A. Experiment Setups

Fig. 6, Fig. 7 and TABLE II show a picture and detail specifications of the experiment platform. The platform adopts a 1.5kW PMSM and sets the operation speed at 1000 rpm. The FOC algorithms are implemented in a TMS320F28335 MCU from Texas Instruments. Furthermore, as illustrated in Fig. 7, our experimental setup constructs cyber-attack scenarios within a controlled, emulated environment to safeguard the hardware. This setup involves embedding predefined malicious code into the motor drive's digital control units based on the adversary resource model. This code establishes a backdoor that can be triggered through a debugging mode by an upper-level computer connected to a public network. Simulated attackers execute the attack by compromising these upper-level computers and activating the backdoor. Simultaneously, a data collection system meticulously records all sensor signals, enabling the comprehensive acquisition and analysis of system data during the simulated attacks. Both case studies assume

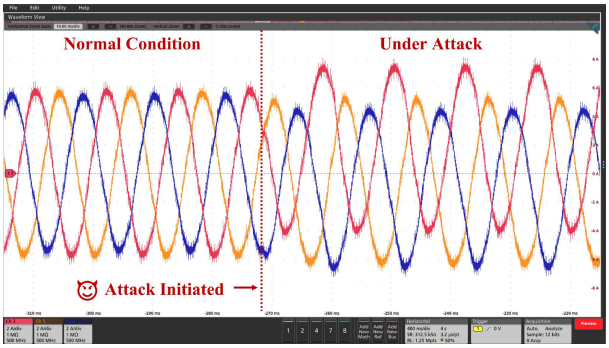


Fig. 8. Three-phase motor line current waveforms of the PMSM with an FDI attack on phase-A ADC offset variable (case 1). The attack policy follows $\hat{s} = s + \alpha$ with $\alpha = 0.1$.

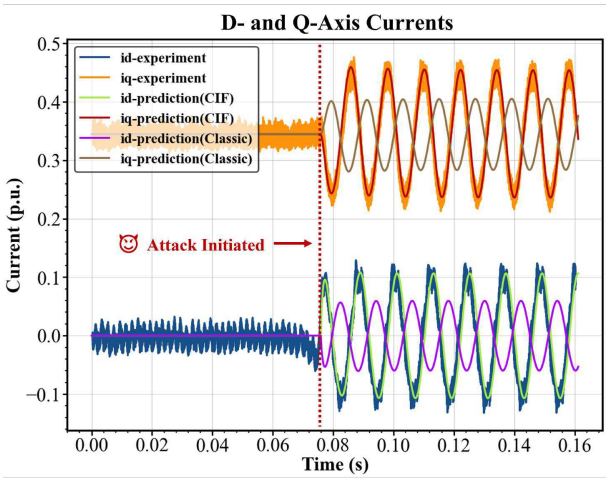


Fig. 9. D- and Q-Axis current waveforms from the experiment, the CIF model prediction, and the traditional analysis predictions with no extra information of case 1 attack ($\alpha = 0.1$).

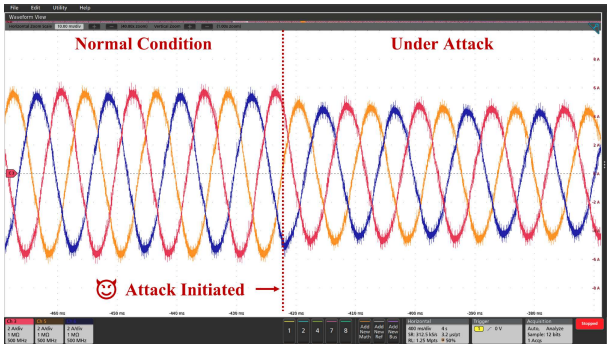


Fig. 10. Three-phase motor line current waveforms of the PMSM with an FDI attack on speed feedback (case 2). The attack policy follows $\hat{s} = s + \alpha$ with $\alpha = 0.1$.

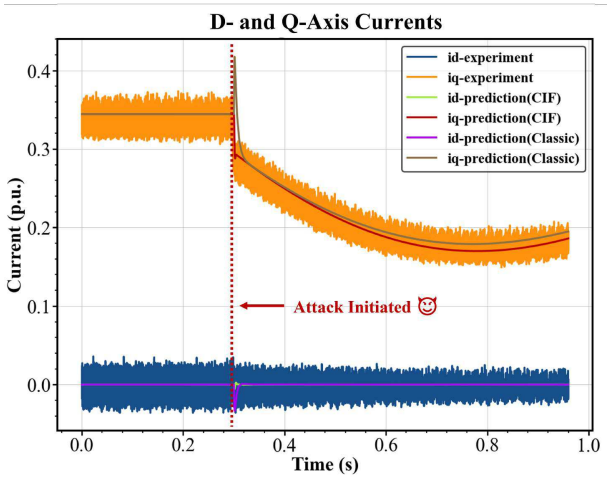


Fig. 11. D- and Q-Axis current waveforms from the experiment, the CIF model prediction, and the traditional analysis model predictions of case 2 attack ($\alpha = 0.1$).

that the attack lasts 1 second before the system detects and clears it. In addition, impact metrics are automatically calculated once the attack is removed.

B. Case 1: FDI attack on the motor current offset variable

Fig. 8 depicts motor line current waveforms during the attack, following the policy shown in Eq. (14) with α as shown. The attack induces imbalanced motor currents, leading to torque oscillations and vibrations. Fig. 9 shows the D- and Q-axis current waveforms after transforming the raw current data to the DQZ frame. It also adds the predicted D- and Q- axis currents from tainted state trajectories (section III) for comparison, showing high accuracy. Additionaly, Fig. 9 presents results from the traditional analysis model, assuming direct addition of the attack policy to the phase current feedback signal. Fig. 9 also includes results from the traditional model, assuming direct addition of the attack policy to the phase current feedback signal. Without additional information, the traditional analysis doesn't consider the attack propagation from ADC calculations to voltage outputs. It treats $x_{offsetA}$ in Eq. (14) as current feedback, resulting in different outcomes, as seen in Fig. 9.

Table. III displays attack impact metrics for various α values. Since the attack initiation time varies, initial phase angles differ across experiments, causing slight variations in the impact metrics. Thus, the table reports the average value from five independent experiments, indicating that the CIF model accurately predicts impact under different attack coefficients.

C. Case 2: FDI attack on motor speed feedback variable

Fig. 10 depicts motor line current waveforms during the attack, targeting speed feedback. Due to the slower mechanical system responses, current waveforms show minimal variations during the attack. This characteristic contributes to the ease with which the Stuxnet worm compromised industrial motor operation speed. Fig. 11 displays current waveforms transformed into the DQZ reference frame linked to the CIF model's predicted trajectories (Section III). These results affirm the CIF model's ability to make precise predictions about the attack's effects.

To highlight the novelty of the CIF model, we consider another scenario involving an FDI attack on speed feedback (case 2), as depicted in Fig. 5 In this case, the attack focuses on

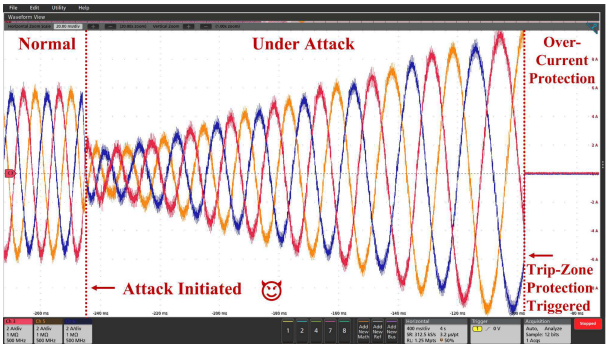


Fig. 12. Three-phase motor line current waveforms of the PMSM in the extended scenario of case 2, where a FDI attack on ω_{mc} in Eq. (48) is implemented. The attack policy follows $\hat{s} = s + \alpha$ with $\alpha = 0.1$.

the speed variable itself, rather than the speed calculation process. In conventional models, these two scenarios might seem equivalent since they both target speed feedback. However, it's important to note that the practical systems often include a small low-pass filter in the speed calculation process, as shown in Eq. (48). Here K_1 and K_2 are the filter coefficients; $\omega_{m(n)}$ and $\omega_{m(n-1)}$ are the current and previous speed feedback; ω_{mc} is the current calculated speed from encoder signals.

$$\omega_{m(n)} = K_1 \cdot \omega_{mc} + K_2 \cdot \omega_{m(n-1)} \tag{48}$$

Because of this filter, the speed calculation process needs to update $\omega_{m(n-1)}$ after every control cycle. Therefore, if the attack is targetting $\omega_{m(n)}$ before the update or is targetting ω_{mc}, the injected bias will integrate at a fast pace. Such an integrated bias then leads to the saturation of the speed PI regulator. The tainted voltage output will ultimately cause unstable motor line currents and trigger the pre-defined over-current protection.

Fig. 12 shows the current waveforms in such a scenario. The ubiquity of the complex behaviors described above presents significant challenges for unilateral defense strategies due to their inherent simplifications. These strategies often fail to effectively address a range of sophisticated cyber threats, including buffer-overflow attacks, malicious overrun attacks, Denial of Service (DOS) attacks, and various forms of False Data Injection (FDI) attacks. As such, it becomes essential to integrate insights from both cyber and physical domains, thereby fostering the development of a more comprehensive and effective analysis framework. Consequently, our proposed security model significantly advances beyond traditional analysis models, particularly in addressing the complexities of these practical scenarios. Then, the attack impact metrics associated with different α are shown in Table. IV. Similar to the previous case study, the experiment attack impact index in Table. IV is the average value among five independent experiments. The results again suggest that the CIF model could accurately predict the impact of this attack with different attack coefficients.

In conclusion, the advancement of the proposed security model can be summarized as follows:

1) It links real-world cyber vulnerabilities to power electronics control models.
2) It accurately predicts the impact of attacks on electric machine drives stemming from various vulnerable onboard resources, like register data and calculation procedures.
3) The CIF model provides crucial internal controller structure information, enhancing practical applicability.

TABLE III
CASE 1 IMPACT METRICS

α	pred. $\mathcal{I}_1$	pred. $\mathcal{I}_2$	expe. $\mathcal{I}_1$	expe. $\mathcal{I}_2$
-0.30	0.0045	0.1924	0.0044	0.1931
-0.25	0.0037	0.1602	0.0036	0.1599
-0.20	0.0028	0.1281	0.0025	0.1273
-0.15	0.0022	0.0960	0.0019	0.0954
-0.10	0.0013	0.0641	0.0011	0.0634
-0.05	0.0008	0.0320	0.0009	0.0329
0.05	0.0007	0.0320	0.0010	0.0314
0.10	0.0017	0.0638	0.0020	0.0628
0.15	0.0019	0.0961	0.0018	0.0968
0.20	0.0029	0.1283	0.0032	0.1281
0.25	0.0033	0.1594	0.0032	0.1605
0.30	0.0051	0.1921	0.0049	0.1912

TABLE IV
CASE 2 IMPACT METRICS

α	pred. $\mathcal{I}_1$	pred. $\mathcal{I}_2$	expe. $\mathcal{I}_1$	expe. $\mathcal{I}_2$
-0.150	0.2955	0.2883	0.2952	0.2891
-0.125	0.2462	0.2402	0.2450	0.2410
-0.100	0.1970	0.1922	0.1977	0.1925
-0.075	0.1477	0.1441	0.1475	0.1426
-0.050	0.0985	0.0961	0.0953	0.9745
-0.025	0.0492	0.0481	0.0491	0.0479
0.025	0.0492	0.0481	0.0487	0.0500
0.050	0.0985	0.0961	0.0989	0.0948
0.075	0.1477	0.1441	0.1490	0.1439
0.100	0.1970	0.1922	0.1951	0.1937
0.125	0.2462	0.2402	0.2471	0.2401
0.150	0.2955	0.2883	0.2941	0.2885

Additionally, the proposed framework offers significant benefits for practical applications. Firstly, it provides system designers with valuable information to evaluate vulnerabilities and enhance security designs. This aspect is particularly critical in the iterative process of strengthening system defenses. Secondly, as data-driven attack detection and diagnostics gain increasing prominence, our framework serves as a valuable tool for generating reliable datasets representing potential cyber-threats. This contribution is especially important given the scarcity of real-world data on such threats in power electronics and related fields.

V. CONCLUSIONS

This paper bridges the gap between security analysis in computer science and system impact analysis using traditional control models. It introduces a novel security model for digitally controlled electric machine drives that connects real-world system vulnerabilities to the system state-space model through the innovative CIF model. By incorporating informatics and taint graph analysis with traditional control diagrams, the CIF model effectively traces the path of attack propagation from adversary resources to controller outputs. Experimental results validate the model's ability to uncover attack propagation and accurately predict their impacts.

REFERENCES

[1] S. Collins and S. McCombie, "Stuxnet: the emergence of a new cyber weapon and its implications," *Journal of Policing, Intelligence and Counter Terrorism*, vol. 7, no. 1, pp. 80–91, 2012.

[2] T. Ring, "Connected cars–the next targe tfor hackers," *Network Security*, vol. 2015, no. 11, pp. 11–16, 2015.

[3] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*. IEEE, 2017, pp. 1–8.

[4] V. K. Kukkala, S. V. Thiruloga, and S. Pasricha, "Roadmap for cybersecurity in autonomous vehicles," *IEEE Consumer Electronics Magazine*, vol. 11, no. 6, pp. 13–23, 2022.

[5] B. Zhu and S. Sastry, "Scada-specific intrusion detection/prevention systems: a survey and taxonomy," in *Proceedings of the 1st workshop on secure control systems (SCS)*, vol. 11, 2010, p. 7.

[6] C. Yulia, B. Pete, B. Andrew, E. Peter, J. Kevin, S. Hugh, and S. Kristan, "A review of cyber security risk assessment methods for scada systems," *Computers & Security*, vol. 56, pp. 1–27, 2016.

[7] B. Canaan, B. Colicchio, and D. Ould Abdeslam, "Microgrid cybersecurity: Review and challenges toward resilience," *Applied Sciences*, vol. 10, no. 16, p. 5649, 2020.

[8] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Computers & Security*, vol. 89, p. 101677, 2020.

[9] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[10] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, pp. 1–36, 2018.

[11] B. Yang, J. Ye, and L. Guo, "Fast detection for cyber threats in electric vehicle traction motor drives," *IEEE Transactions on Transportation Electrification*, vol. 8, no. 1, pp. 767–777, 2022.

[12] L. Guo, B. Yang, J. Ye, J. M. Velni, and W. Song, "Attack-resilient lateral stability control for four-wheel-driven evs considering changed driver behavior under cyber threats," *IEEE Transactions on Transportation Electrification*, vol. 8, no. 1, pp. 1362–1375, 2022.

[13] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2002, pp. 2–12.

[14] S. Hounsinou, M. Stidd, U. Ezeobi, H. Olufowobi, M. Nasri, and G. Bloom, "Vulnerability of controller area network to schedule-based attacks," in *2021 IEEE Real-Time Systems Symposium (RTSS)*, 2021, pp. 495–507.

[15] S. Jafarnejad, L. Codeca, W. Bronzi, R. Frank, and T. Engel, "A car hacking experiment: When connectivity meets vulnerability," in *2015 IEEE Globecom Workshops (GC Wkshps)*, 2015, pp. 1–6.

[16] Z. Drias, A. Serhrouchni, and O. Vogel, "Taxonomy of attacks on industrial control protocols," in *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)*, 2015, pp. 1–6.

[17] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Vulnerability assessments of electric drive systems due to sensor data integrity attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3301–3310, 2020.

[18] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber-physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, pp. 4639–4657, 2021.

[19] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (cpps): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151 019–151 064, 2020.

[20] T. H. Austin and C. Flanagan, "Efficient purely-dynamic information flow analysis," in *Proceedings of the ACM SIGPLAN Fourth Workshop on Programming Languages and Analysis for Security*, 2009, pp. 113–124.

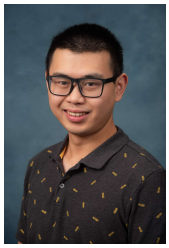
[21] A. Sabelfeld and A. C. Myers, "Language-based information-flow security," *IEEE Journal on selected areas in communications*, vol. 21, no. 1, pp. 5–19, 2003.

[22] J. Ming, D. Wu, G. Xiao, J. Wang, and P. Liu, "{TaintPipe}: Pipelined symbolic taint analysis," in *24th USENIX Security Symposium (USENIX Security 15)*, 2015, pp. 65–80.

[23] G. Mazzarolo and A. D. Jurcut, "Insider threats in cyber security: The enemy within the gates," *arXiv preprint arXiv:1911.09575*, 2019.

[24] N. Gupta, A. Tiwari, S. T. Bukkapatnam, and R. Karri, "Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks," *IEEE Access*, vol. 8, pp. 47 322–47 333, 2020.

[25] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, 2011, pp. 4490–4494.



Bowen Yang (IEEE S'18-M'23) received his B.Sc. degree from Huazhong University of Science and Technology in Wuhan, China, in 2018. Following this, he pursued his Ph.D. at the University of Georgia in Athens, GA, USA, completing his degree in 2023. Throughout his time at the University of Georgia, Bowen served as a Research Assistant and contributed to multiple research projects. Currently, he is a graduate intern at the National Renewable Energy Laboratory (NREL), where he continues his work in power electronics and electric machines. Bowen's research interests include advanced control for power electronics and electric machines, inverter-based resources (IBRs) based power systems, cyber-physical systems, machine learning, and their applications in electric vehicles, microgrids, and manufacturing systems.

He Yang (IEEE S'23) received the B.S. in electrical engineering from Tianjin University, Tianjin, China in 2018. He received the M.S. degrees in electrical engineering from the University of New South Wales, Sydney, Australia, in 2023. He is currently pursuing the Ph.D. degree with the University of Georgia, Athens, GA, USA, where he is also a Research Assistant. His recent research focuses on cyber-physical security of power electronics and electric drive systems.

Jin Ye (IEEE S'13-M'14-SM'16) received the B.S. and M.S. degrees in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 2008 and 2011, respectively. She also received her Ph.D. degree in electrical engineering from McMaster University, Hamilton, Ontario, Canada in 2014. She is currently an associate professor of electrical engineering and the director of the Intelligent Power Electronics and Electric Machines Laboratory at the University of Georgia. She has received a creative research medal for her significant contributions to power electronics security field and received a best paper award from IEEE Applied Power Electronics Conference. She is a general chair of 2019 IEEE Transportation Electrification Conference and Expo (ITEC). She has served in the organizing committee of IEEE Energy Conversion Congress and Expo (ECCE) since 2019 as a publication chair and woman in engineering (WIE) chair. She is a secretary for IEEE power electronics society (PELS) Technical Committee on Transportation Electrification (TC 4). She is an associate editor for IEEE Transactions on Power Electronics, IEEE Open Journal of Power Electronics, IEEE Transactions on Vehicular Technology and IEEE Transactions on Industry Applications. She was an associate editor for IEEE Transactions on Transportation Electrification 2017-2020. Her main research areas include power electronics, electric machines, smart grids, electrified transportation, and cyber-physical security.