Vulnerability Assessments of Electric Drive Systems Due to Sensor Data Integrity Attacks

Bowen Yang, Lulu Guo, Fangyu Li, Jin Ye, *Senior Member, IEEE*, and Wenzhan Song

***Abstract*—In this article, a systematic and generalized methodology is originally proposed to assess the vulnerability of electric drive systems due to sensor data integrity attacks. Novel evaluation metrics from the perspectives of steady-state and transient performance of electric drive systems are established to evaluate the system condition under different attacks. By using these metrics, innovative index-based resilience and security criteria, together with the stability theorem, are proposed specifically for electric drive systems, which can then be used for cyber-attack detection and diagnosis in a more systematic manner. Then, based on the simulation results under 15 attack cases (five typical types), the qualitative attack impacts on the dynamic characteristics and the statistical damage of different cyber-attacks to the defined metrics are analyzed, which can serve as useful guidelines for attack detection, diagnosis, and countermeasures.**

***Index Terms*—Cyber-physical system, cyber security, electric drive system, industrial system.**

I. Introduction

RECENT years have witnessed a significant development in cyber-physical systems, which has permeated modern industrial systems, including energy production, power electronics, manufacturing, and automotive industry [1]. However, a large number of communication and complex networks also brings cyber security concerns [2], [3]. Especially, for the electric systems (like power grids, wind farms, and electric vehicles), as a huge amount of energy contained in the power equipment is fully controlled by networked electronic units, the systems are directly exposed to cyber threats. Once the attackers have compromised any of the controllers without being detected, catastrophic damages are usually inevitable. For instance, on August 14, 2003, a large-scale electric power blackout occurred in North America, which was caused by a software program failure in the power system, and this events affected around 50 million people and 61 800 MW of electric loads [4]. In 2010, a computer worm "Stuxnet" was discovered targeting Siemens industrial software and equipment to unstable the power system operation [5], [6]. In addition to power systems, electric drive systems, which are playing an increasingly important role in industrial applications, can also be attacked through maliciously modifying controller in real-life applications. In 2015, an unnamed steel mill in Germany was attacked. The hackers were reported to maliciously manipulate the control system such that a blast furnace could not be properly shut down, resulting in unspecified massive damage. This is the second confirmed case of a cyber-physical attack that caused physical destruction of equipment after Stuxnet [7]. Most recently, in March 2019, hackers in Tencent Keen Security Lab attacked Tesla's autopilot and manipulated the control of the vehicle that is powered by electric drive systems. This cyber-attack can have serious consequences, such as causing the electric vehicle to suddenly switching lanes [8]. In August 2019, security researchers found a zero-day vulnerability in a popular building controller used for managing various systems, including heating, ventilation, and air conditioning (HVAC) [9], and they were able to maliciously modify the controller such as through modifying sensors (for instance, temperature sensors). This will later adversely impact HVAC systems, which are primarily electric drive systems. Therefore, electric drive systems are vulnerable to a variety of cyber-attacks, including sensor data integrity attack we study in this article. These cyber-attack events have received an increasing concern, but have not yet been addressed in many industrial applications. Realistically, manufacturers may implant trojans in the controllers, or attackers may initiate the port scan to find the weak point in cyber networks and implant a malware for data integrity attacks. Therefore, we consider a general electric drive system shown in Fig. 1, which is vulnerable to a variety of cyber-attacks. We use attack vectors denoted in red to represent potential cyber-attacks on electric drive systems. For example, local sensor signals could be modified or blocked to make the system unstable (attack A), or control signals from higher level controllers could be delayed or fabricated to lower the system efficiency (attack C), or even more malicious attacks could target on the switching signals to make power modules nonfunctional (attack D), etc.

To address these cyber-attack issues on electric systems, cyber security has received increasing attention, and much effort has been devoted to vulnerability assessment, cyber-physical attack detection, and resilient control. In the field of smart grids, Sridhar and Manimaran [10] analyzed the data integrity attacks on automatic generation control loop. In [11], the cyber security policies for flexible alternating current transmission

Manuscript received August 18, 2019; accepted September 25, 2019. Date of publication October 17, 2019; date of current version February 6, 2020. This work was supported in part by the National Science Foundation under Grant ECCS-1946057 and in part by Southern Company. Paper no. TII-19-3802. *(Corresponding author: Jin Ye.)*

The authors are with the Center for Cyber-Physical Systems, University of Georgia, Athens, GA 30602 USA (e-mail: bowen.yang@uga.edu; lulu.guo@uga.edu; fangyu.li@uga.edu; jin.ye@uga.edu; wsong@uga.edu).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2019.2948056

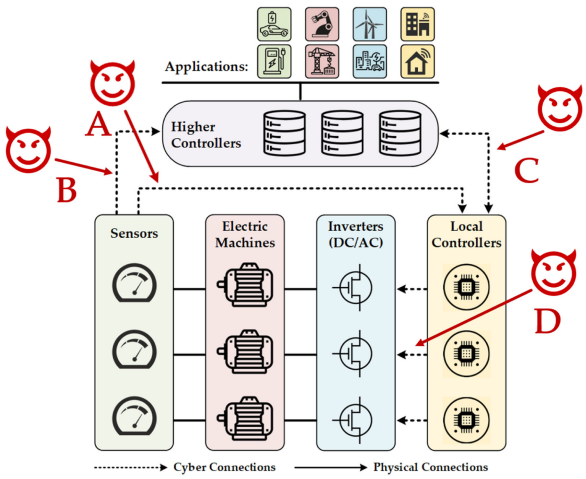


Fig. 1. General diagram of the electric drive systems.

devices are discussed. In [12] and [13], intrusion detection methods are proposed for advanced metering infrastructures and power system operations. In [14] and [15], advanced data processing approaches (e.g., data mining and neural network) are used to detect and classify different cyber-attacks targeting on smart grids. With regard to vulnerability assessment, Xie *et al.* [16] presented the impact of integrity attacks on electric market operations, Esfahani *et al.* [17] used reachability methods in graph theory to assess the risks and vulnerabilities of two-area power systems, and Ten *et al.* [18] proposed the attack and defense modeling for critical cyber infrastructures. In addition, in [19]–[21], methods of assessment, detection, and possible countermeasures for process control systems have been researched.

However, cyber security works in smart grids and critical infrastructure are mostly focused on the system level; to the best of our knowledge, to date, no works have been developed for device-level cyber security in electric drive systems, which are an important and vulnerable part of industrial environments (e.g., electric vehicle, intelligent manufacturing, renewable energy, and smart city). Fig. 1 shows a general diagram of the electric drive systems with a large number of information exchanges between sensors and local/higher controllers, which are vulnerable to cyber and physical threats. Although some methods for smart grids can be effective in addressing some types of cyber-attacks, they can hardly be applied to electric drive systems directly. The reasons are as follows: 1) existing resilient control methodologies for smart grids mainly focus on few metrics such as active (or reactive) power, system frequency, node voltage, and power angle, which may be unfeasible for electric drive systems; and 2) the power equipment (like generators, motors, transformers, and transmission lines) are often modeled as voltage sources, impedance, or electric power loads in power grids to simplify vulnerability assessment, since only stability, efficiency, and economic performances of the grid are of concern. However, in electric drive systems, more detailed models (device and system) and different metrics should be considered to evaluate the system comprehensively. For example, an electric vehicle requires fast and accurate tracking of the torque and speed references to ensure dynamic performance, low torque ripple to reduce mechanic vibrations and noise, low-current total harmonics distortion, and high power factor to extend the life cycle of battery packs, as well as minimizing power losses to enhance the driving range. Therefore, it is essential and important to emphasize the cyber security challenge of the electric drive systems, and novel methodologies of vulnerability assessment, detection, and resilient control should be developed. Among these works, in this article, we present, first, a systematic methodology to assess the vulnerability of electric drive systems due to sensor data integrity attacks. The contributions are as follows.

1) Novel evaluation metrics specific to electric drive systems are established to evaluate the system condition under a variety of sensor data integrity attacks, including more realistic and sophisticated attacks.
2) Together with the stability theorem, innovative index-based resilience and security criteria are proposed specifically for electric drive systems by considering the nonlinear characteristics, which can then be used for cyber-attack detection and diagnosis in a more systematic manner.
3) The qualitative attack impact on the dynamic performance and the statistical results of impact index due to different cyber-attacks are analyzed, which can serve as useful guidelines for attack detection, diagnosis, and countermeasures.

The rest of this article is organized as follows. In Section II, the cyber-physical model of electric drive system is introduced. The evaluation metrics are discussed in Section III. Then, Section IV focuses on the mathematical modeling of typical sensor integrity attacks. In Section V, stability, security, and resiliency analysis, simulation results under different integrity attacks, and vulnerability assessments are given. Finally, Section VI concludes this article.

II. Cyber-Physical Modeling of the IPM-Based Electric Drive System

Fig. 2 shows the cyber-physical model of an interior permanent magnetic synchronous machine (IPM)-based electric drive system. In the physical part, the battery packs and dc–dc converter form the dc power supply, which can provide the power input to the dc–ac inverter. Then, the inverter drives the IPM under the control of the pulsewidth modulation (PWM) signals, which are generated by the local controller (S_1–S_6). Sensors are implemented on the inverter output ports and sample the three-phase currents of the electric machine windings. The cyber system is mainly in charge of receiving and processing the sensor signals, generating the PWM control signals, and communicating with higher level controllers.

A. IPM Models

IPM is currently widely adopted in the applications of electric vehicles. Under the traditional three-phase static reference frame, the electrical relationships in each phase could

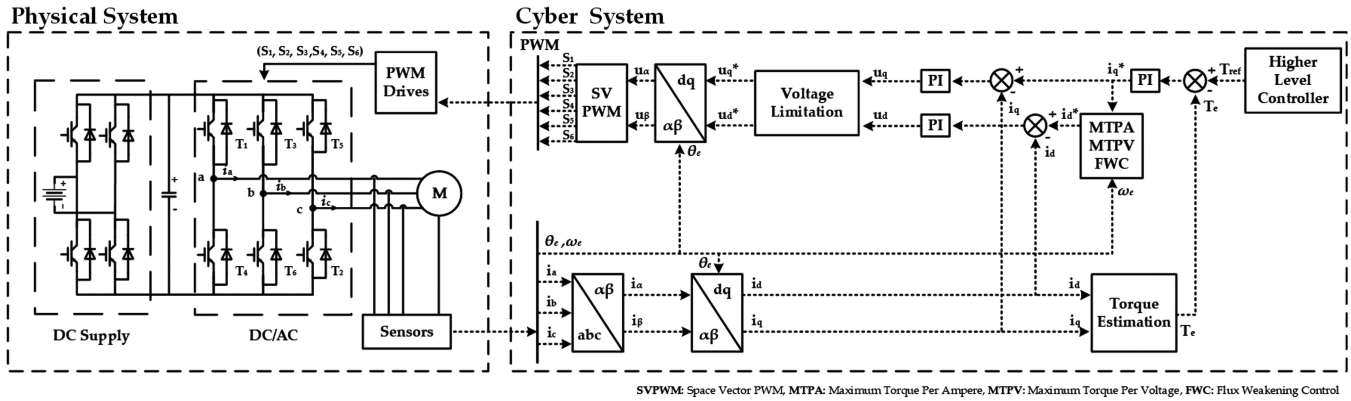


Fig. 2. Cyber-physical model of the IPM-based electric drive system.

be described as

$$\mathbf{v} = \mathbf{R}\mathbf{i} + \frac{d}{dt}\mathbf{\Lambda},\ \mathbf{\Lambda} = \mathbf{L}\mathbf{i} \tag{1}$$

with

$$\mathbf{L} = \begin{bmatrix} L_{aa} & L_{ab} & L_{ac} & L_{af} \\ L_{ba} & L_{bb} & L_{bc} & L_{bf} \\ L_{ca} & L_{cb} & L_{cc} & L_{cf} \\ L_{fa} & L_{fb} & L_{fc} & L_{ff} \end{bmatrix} \tag{2}$$

where voltage vector $\mathbf{v} = [v_a, v_b, v_c, v_f]^T$, current vector $\mathbf{i} = [i_a, i_b, i_c, i_f]^T$, flux linkage vector $\mathbf{\Lambda} = [\Lambda_a, \Lambda_b, \Lambda_c, \Lambda_f]^T$, and winding resistance matrix $\mathbf{R} = \text{diag}[R_a, R_b, R_c, R_f]$. $\mathbf{L}$ is the inductance each phase. More specifically, the flux linkage $\Lambda_f = \Lambda_{pm}$ is produced by the magnet mounted in the rotor; v_f, i_f, and R_f represent the equivalent excitation voltage, current, and resistance, respectively; L_{fx} and $L_{xf}, x = a, b, c$, reflect the flux linkage in each phase provided by the rotor magnet.

To simplify the analysis, direct-quadrant-zero (DQZ) transformation is adopted to transfer the variables in the stator static reference frame to the rotor rotating reference frame. Then, the results could be described as follows:

1) flux linkage:

$$\begin{cases} \Lambda_d = L_d i_d + \Lambda_{pm} \\ \Lambda_q = L_q i_q \end{cases} \tag{3}$$

2) voltage:

$$\begin{cases} v_d = R_s i_d + L_d \frac{di_d}{dt} - \omega_e L_q i_q \\ v_q = R_s i_q + L_q \frac{di_q}{dt} + \omega_e L_d i_d + \omega_e \Lambda_{pm} \end{cases} \tag{4}$$

3) torque:

$$T_e = \frac{3}{2} p[\Lambda_{pm} i_q + (L_d - L_q) i_d i_q] \tag{5}$$

where L_d and L_q are the inductance of d-axis and q-axis, ω_e is the electrical angular speed, p is the number of pole pairs, and R_s is the equivalent winding resistance in the DQ reference frame. It should be noted that when the stator winding is connected in the "Y" model, the zero component will always be 0, as suggested by Kirchhoff's law. That is the reason why the zero component is not included in the DQ model described above.

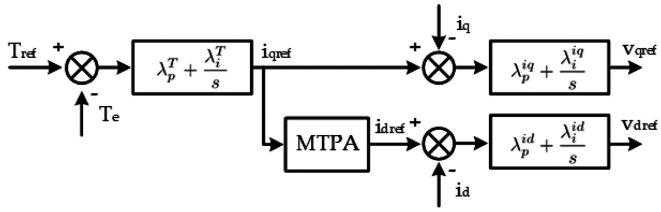


Fig. 3. Control diagram of three PI controllers.

B. Proportional–Integral Controllers

Proportional–integral (PI) controllers are one of the most widely used controllers in the industrial environment, so the electric drive system researched in this article adopts three PI controllers, as shown in Figs. 2 and 3, to regulate the error between the reference and the actual torque and d-axis and q-axis current.

C. Reference Current Vector Optimization

As shown in Fig. 3, the reference current vector $[i_d, i_q]^T$ is selected to track the torque command. To achieve the maximum system efficiency while producing the same torque, a widely implemented algorithm, maximum torque per ampere (MTPA), is adopted to optimize the current vectors. The diagram of the optimization is shown in Fig. 4, where the blue circle denotes the current limits and the red ellipse is the voltage limits; the yellow and green trajectories are MTPA and maximum torque per voltage (MTPV), respectively; the purple trajectory defines the constant torque profile. Detailed procedures of the algorithm are described as follows.

1) If the system is operating with a speed lower than the basic speed ω_b, the reference current vector should follow the MTPA trajectory defined by

$$i_{d\text{ref}} = \frac{\Lambda_{pm}}{2(L_q - L_d)} - \sqrt{\frac{\Lambda_{pm}^2}{4(L_q - L_d)^2} + i_{q\text{ref}}^2}. \tag{6}$$

2) If the speed is higher than ω_b but lower than ω_2, the reference current vector should follow the MTPA trajectory, while the vector is inside the voltage limit. Otherwise, if

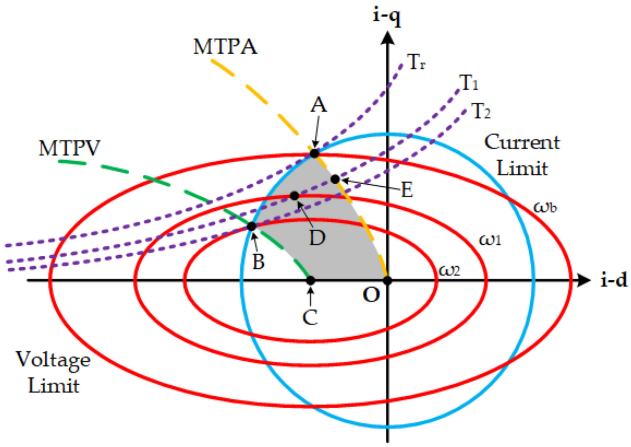


Fig. 4. Diagram of the reference current vector optimization.

the vector is outside the voltage limit, such as point E, the current vector should be selected by the flux-weakening control as

$$i_{d\text{ref}} = -\frac{\Lambda_{pm}}{L_d} + \frac{1}{L_d}\sqrt{\left(\frac{V_{s\max}}{\omega_e}\right)^2 - (L_q i_{q\text{ref}})^2} \quad (7)$$

denoted as point D in the figure.

3) If the speed is higher than ω_2, the reference current vector should follow the MTPA trajectory, while the vector is inside the voltage limit ellipse. Otherwise, the current vector should follow the MTPV trajectory defined by

$$(L_d - L_q)\left[\left(\frac{L_d i_{d\text{ref}} + \Lambda_{pm}}{L_q}\right)^2 - i_{q\text{ref}}^2\right] + \Lambda_{pm}\left(\frac{L_d i_{d\text{ref}} + \Lambda_{pm}}{L_q}\right) = 0. \quad (8)$$

Generally speaking, the gray region in Fig. 4 (OABC) is where the optimal reference current vector should be selected.

III. Evaluation Metrics

In order to provide an insight into the impact of sensor attacks on the system, as well as to give a guideline for developing monitoring and detection methodology, we propose to use a series of new metrics below. To obtain the transient process of the attack, all metrics are calculated within a sliding window, denoted as $\mathscr{T}_w$.

A. Torque Ripple and Speed Ripple

The torque and speed ripple (marked as S_1 and S_2, respectively) reflect the mechanical characteristics, which are of vital importance to an electric drive system. Large torque or speed ripple can normally bring damages to the mechanical components such as rotor and shaft and can lead to other negative consequences like drive performance discomfort in electric vehicles and poor motion accuracy in manufacturing and servo systems. The two indices are defined as

$$S_1(t_0) = \frac{\max\{T(t)\} - \min\{T(t)\}}{\text{ave}\{T(t)\}}$$
$$S_2(t_0) = \frac{\max\{n(t)\} - \min\{n(t)\}}{\text{ave}\{n(t)\}} \quad (9)$$

where $t \in [t_0, t_0 + \mathscr{T}_w]$; T and n are the electromagnetic torque and the rotating speed, respectively.

B. Current Distortion Index

The current distortion index S_3 is defined to show the degree of current distortion caused by the attack, expressed as

$$S_3 = \sqrt{\frac{\int_{-\infty}^{f_l} I^2(f)df + \int_{f_u}^{+\infty} I^2(f)df}{\int_{f_l}^{f_u} I^2(f)df}} \quad (10)$$

where $I(f)$ is the amplitude of the phase current in the frequency domain after the Fourier Transformation. As harmonics apart from operating frequency may lead to damage to hardware devices such as battery packs and insulated-gate bipolar transistors in the inverter, the distortion should be maintained as low as possible. The dominant current frequency is found to fluctuate around the operating point, and thus, a frequency band $[f_l, f_u]$ is introduced here to differentiate the normal frequency fluctuation and the current distortion caused by attacks, defined by

$$f_u = f_0 + \Delta f,\ f_l = f_0 - \Delta f. \quad (11)$$

Here, f_0 is the operating frequency calculated from the average speed, and Δf denotes the bandwidth.

C. Torque Tracking Error

The torque tracking error, due to the ability to depict the dynamic response characteristic, is normally defined to measure the torque tracking performance and determine whether the system is working at desired operating point. It is defined by

$$S_4 = \frac{\sqrt{\frac{1}{\mathscr{T}_w}\int_{t_0}^{t_0+\mathscr{T}_w}(T_{\text{ref}}(t) - T_e(t))^2 dt}}{\text{ave}\{T_{\text{ref}}(t)\}} \quad (12)$$

where T_{ref} is the torque reference; T_e denotes actual torque, which could be directly measured or calculated by the phase current.

D. Three-Phase Current Unbalance Components

The three-phase current unbalance components are calculated by the asymmetric components methods, which reflect the asymmetry features among three-phase currents. The detailed calculating procedure is shown in Fig. 5, wherein $[\mathbf{N} - \mathbf{Park}]$ is the Park transformation matrix in the negative sequence; LPF represents the low-pass filter and is derived by

$$G(s) = \frac{(2\pi \cdot f)^2}{(s + 2\pi \cdot f)^2} \quad (13)$$

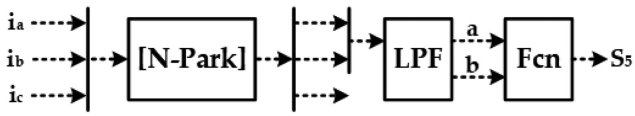


Fig. 5. Calculation procedure of S_5.

where f is the cutoff frequency. Then, the index S_5 is the amplitude of the unbalance components, calculated by

$$S_5 = \sqrt{a^2 + b^2}. \tag{14}$$

The unbalance current will bring a great damage to the system, even leading to instability. Normally, if the system is on healthy condition, the unbalance components are approximately zero; if not, there probably exist some attacks or faults.

E. Impact Index

As these five metrics describe different characteristics of the electric drive system, a more general impact index $\mathcal{K}_{\text{imp}}$ is proposed for the purpose of comprehensive assessment. The calculation of $\mathcal{K}_{\text{imp}}$ is shown as

$$\mathcal{K}_{\text{imp}} = \sum_{x=1}^{5} k_{\text{imp}}^{S_x} \tag{15}$$

where $k_{\text{imp}}^{S_x}$ is the impact factor for each evaluation metrics. The calculation expression is shown as

$$k_{\text{imp}}^{S_x} = \left(\frac{k_x^{\text{attack}} + k_x^{\text{after-attack}}}{k_x^{\text{normal}}} - 2 \right) \tag{16}$$

where k_x^{attack}, $k_x^{\text{after-attack}}$, and k_x^{normal} are the root mean square of S_1–S_5 during the attack period, beyond attack period, and the normal period, respectively. The detailed calculation process is shown as

$$\begin{aligned} k_x^{\text{attack}} &= \sqrt{\frac{1}{\mathcal{T}_{\text{attack}}} \int_{\mathcal{T}_{\text{attack}}} S_x^2 dt} \\ k_x^{\text{normal}} &= \sqrt{\frac{1}{\mathcal{T}_{\text{normal}}} \int_{\mathcal{T}_{\text{normal}}} S_x^2 dt}. \\ k_x^{\text{after-attack}} &= \sqrt{\frac{1}{\mathcal{T}_{\text{after-attack}}} \int_{\mathcal{T}_{\text{after-attack}}} S_x^2 dt} \end{aligned} \tag{17}$$

where $\mathcal{T}_{\text{attack}}, \mathcal{T}_{\text{after-attack}}$, and $\mathcal{T}_{\text{normal}}$ are the different time periods.

IV. Attack Modeling

To quantitatively analyze the impact of cyber-attacks on electric drive systems, we suppose the real and fake feedback measurements denoted as y and $\hat{y}$, respectively, and the time horizon under attack is $\mathbf{T_{ATK}} = [t_0, t_0 + T_a]$. Then, two common attacks are modeled as

$$\hat{y} = \begin{cases} y, & (t \notin \mathbf{T_{ATK}}) \\ \alpha \cdot y, & (t \in \mathbf{T_{ATK}}) \end{cases} \tag{18}$$

$$\hat{y} = \begin{cases} y, & (t \notin \mathbf{T_{ATK}}) \\ y + \beta, & (t \in \mathbf{T_{ATK}}) \end{cases} \tag{19}$$

where t_0 is the start time of the attack and T_a is the time of attack duration. In the above attack model, α could be greater than 1, meaning that the signal is falsely amplified, or smaller than 1, meaning that the signal is falsely reduced; β could be a constant or a complex function. In this article, β is modeled as three different functions: a white noise injection, a decaying high-frequency harmonics injection, and a periodic pulse injection, which can be expressed as follows:

$$\beta = \text{white noise} \tag{20}$$

which is defined by the energy and sampling time

$$\beta = Ae^{-t/\tau} \cdot \sin(2\pi \cdot f \cdot t) \tag{21}$$

where A, τ, and f represent the oscillation amplitude, decaying coefficient, and oscillation frequency, respectively

$$\beta = \mathscr{F}(t) = \begin{cases} K & (kT_s \leqslant t < D \cdot T_s + kT_s) \\ 0 & (D \cdot T_s + kT_s \leqslant t < (k+1)T_s) \end{cases} \tag{22}$$

where k is an integer, and D, T_s, and K are the duty cycle, signal period, and attack amplitude, respectively. Based on such attack models, five specific types attacks are established targeting on single phase, two phases, and three phases, which results in 15 cases, as shown in Table I. It should be pointed out that all these 15 cases are not meticulously designed for some specific attack purpose. Nevertheless, they could be used as preliminary demonstrations.

V. Simulation Results and Impact Analysis

To analyze the impact of the attack cases in Table I, a 50-kW IPM-based electric drive system is built in MATLAB Simulink with the same hardware topology and controller diagram shown in Fig. 2. Three main works are presented here.

1) Based on the defined evaluation metrics and control theory, we propose an analytic methodology of evaluating system stability, security, and resilience, and the metric-based boundaries can be used further to detect the malicious attacks online.
2) Qualitative and quantitative impacts of attacks are analyzed in detail, and then, general guidelines are summarized.
3) The statistical graph is shown in the last part, under which we evaluate the potential damage and influence of different types of attacks on the defined metrics, which can serve as guidelines for attack detection and countermeasures in real-life applications.

A. Stability, Security, and Resilience of the System

1) Stability of the System: As the system is a high-order nonlinear system, it is hard to find a proper Lyapunov function to establish the stability criteria. Therefore, to illustrate the system stability, we propose a proposition in a broad sense.

Proposition 1: Given a continuous state space $\mathbf{X} \subseteq \mathbb{R}^n$, if the system has an equilibrium point $\mathbf{X_e}$, and there exists a set $\mathbb{B}^n$,

TABLE I
ATTACK MODELING AND CASE DEFINITION

Case Definition		Attack Targets		
		Phase A	Phase A and B	Phase A, B and C
$\hat{y} = \alpha y$	$\alpha = 0.8$ (type 1)	Case 1	Case 6	Case 11
	$\alpha = 1.2$ (type 2)	Case 2	Case 7	Case 12
$\hat{y} = y + \beta$	$\beta = noise$ (type 3)	Case 3	Case 8	Case 13
	$\beta = 25e^{-t/0.1} \cdot \sin(2\pi \cdot 200 \cdot t)$ (type 4)	Case 4	Case 9	Case 14
	$\beta = \mathscr{F}(t)$ where $K = 30, Ts = 0.001, D = 0.25$ (type 5)	Case 5	Case 10	Case 15

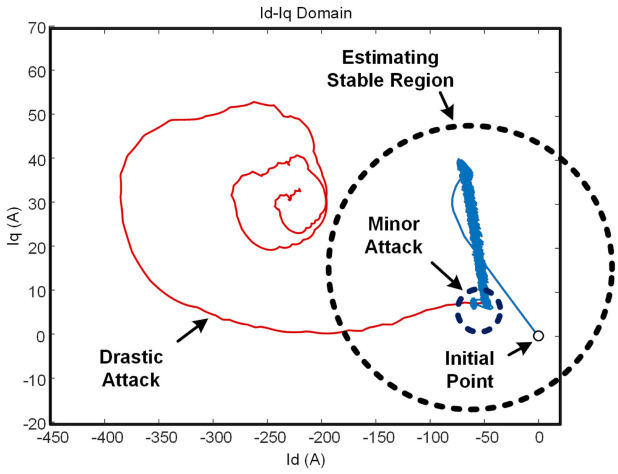


Fig. 6. Phase portrait of i_d and i_q under sensor attacks.

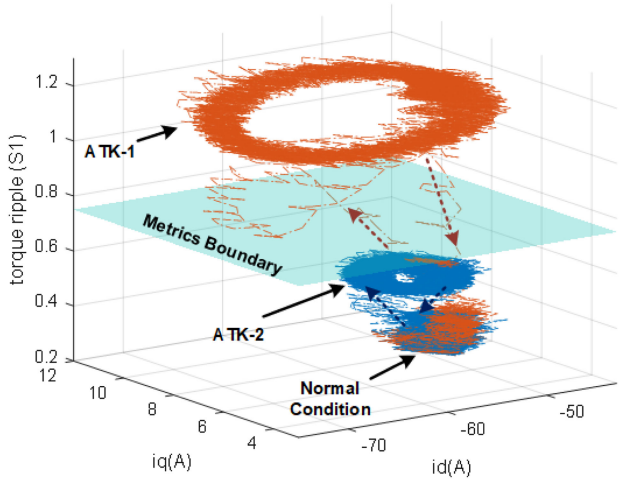


Fig. 7. Metrics boundary in the phase portrait.

which satisfies: 1) $\mathbb{B}^n \subseteq \mathbb{R}^n$; 2) $\mathbf{X_e} \subseteq \mathbb{B}^n$; and 3) for any initial point $\mathbf{X_0} \subseteq \mathbb{B}^n$, the state space $\mathbf{X}$ will eventually converge to the equilibrium point $\mathbf{X_e}$, then the system is stable in $\mathbb{B}^n$, and $\mathbb{B}^n$ is defined as the stable region of the system around the equilibrium point $\mathbf{X_e}$.

Fig. 6 shows the two-dimensional phase portrait (i_d, i_q) of the system. As long as the state-space trajectory of the system belongs to $\mathbb{B}^n$ during the attack, the system will be stable. As shown in Fig. 6, when a minor attack occurs, the deviation from the initial point is quite small, and the whole phase trajectory is inside the boundary $\mathbb{B}^n$, the system is stable; however, if the attack is drastic, as the red trajectory, the operating point will go beyond $\mathbb{B}^n$; thus, the system becomes unstable.

2) Security of the System: To evaluate the security of the system, we define metric-based boundaries as follows.

Proposition 2: Define S_m, $m = 1, 2, 3\ldots$, as a system evaluation metrics. If a boundary $\mathbf{K}_m = [k^m_{\text{lower}}, k^m_{\text{upper}}]$ could be found, which has the following properties: 1) k^m_{lower} and k^m_{upper} is finite; and 2) if $S_m \in \mathbf{K}_m$, the damage caused by the attacks are acceptable, then the system is secure.

Fig. 7 shows the index S_1 under two cyber-attacks. Although the index under $\mathbf{ATK-1}$ can come to the equilibrium range after attack is removed, during the dynamic process, the damage caused by the attacks is not acceptable ($S_1 \notin \mathbf{K}_1$), and thus, the system is not secure.

3) Resilience of the System: The resilience refers to the ability of recovery after suffering from malicious attacks. We consider the recovery time $T_{r,m}$ of the mth index S_m ($m = 1, 2, \ldots$) from the time when the attack is withdrawn to the time when the index restores to its original value. Then, the boundary reflecting the resilience is defined as follows.

Proposition 3: Define $T_{r,m}$, $m = 1, 2, \ldots$, as the system evaluation metrics. If a boundary $\mathbf{T_{r,m}} = [T^{r,m}_{\text{lower}}, T^{r,m}_{\text{upper}}]$ could be found, which has the following properties: 1) $T^{r,m}_{\text{lower}}$ and $T^{r,m}_{\text{upper}}$ is finite; and 2) as long as $T_{r,m} \in \mathbf{T_{r,m}}$, $T_{r,m}$ could restore to its original value when the attack is withdrawn, then the system is resilient.

This boundary represents the resilience performance of the studied electric drive system. The larger boundary demonstrates the better resilience of the systems against cyber-attacks.

4) Remarks: The metric-based boundaries could be obtained through massive simulations or experiments and may vary with different application scenarios. In this subsection, we suppose that the electric drive system is applied to four-wheel-driven electric vehicles. Then, the torque ripple (S_1) boundary could be selected as [0, 0.2] to avoid destroying the yaw stability.

B. Simulation Results Under Sensor Attacks

Based on the evaluation metrics and index introduced in Section III, 15 cases in Table I are simulated and analyzed.

TABLE II
DETAILED SIMULATION RESULTS OF THE IMPACT INDEX

	$k_{imp}^{S_1}$	$k_{imp}^{S_2}$	$k_{imp}^{S_3}$	$k_{imp}^{S_4}$	$k_{imp}^{S_5}$	$\mathcal{K}_{imp}$
1	1.689	14.92	-0.003	1.275	9.521	27.40
2	1.616	14.16	-0.006	0.948	7.427	24.15
3	1.023	4.375	-0.007	0.024	0.088	5.503
4	3.090	6.446	0.034	1.664	3.1781	14.41
5	11.15	31.93	0.226	4.534	3.899	51.74
6	1.995	28.12	0.005	2.014	10.865	43.01
7	1.783	25.41	-0.003	1.448	6.567	35.20
8	1.576	5.086	-0.008	0.059	0.126	6.838
9	2.757	6.263	0.006	1.612	2.663	13.30
10	10.32	29.35	0.087	4.271	3.098	47.12
11	0.471	37.49	0.005	1.940	0.350	40.26
12	0.946	36.25	0.001	1.862	-0.074	38.98
13	-0.048	-0.089	-0.012	-0.225	-0.008	-0.383
14	-0.048	-0.089	-0.012	-0.225	-0.008	-0.383
15	-0.048	-0.089	-0.012	-0.225	-0.008	-0.383

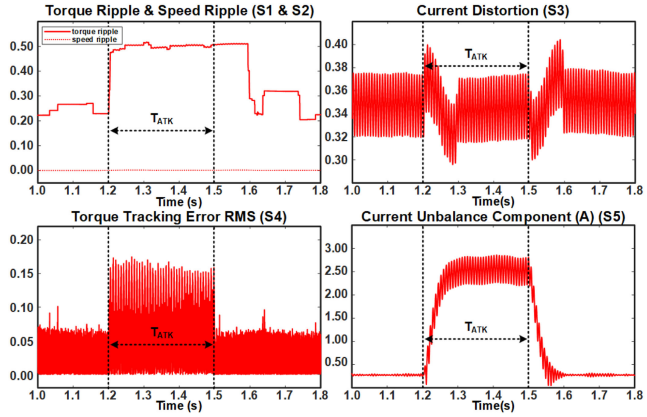


Fig. 8. Case 1: reducing attack, $\hat{y} = 0.8y,\ t \in \mathbf{T_{ATK}}$, targeting phase A.

Table II shows the detailed results of the impact index for each case, which are calculated through (15)–(17). Among these results in Table II, the ones in cases 13–15 are strangely identical. The reason is that in these three cases, sensors of three phases are added by the same false signals, which means all false signals will be transferred to zero-axis component after DQZ transformation. As the control algorithms only adopt d- and q-axis information, false signals in these three cases will not influence the controller performance. Meanwhile, besides these three, we present several cases for better observation, and a sliding window is constructed on the time axis. The trajectories are plotted in Figs. 8–13. It should be pointed out that due to the simple relationship between torque and rotation speed in this model and the similarity between the profiles of S_1 and S_2, these two metrics are drawn in one figure, for the space-saving purpose. Besides, current distortion S_3 is calculated from phase A current, which is always one of the attack targets in the simulation.

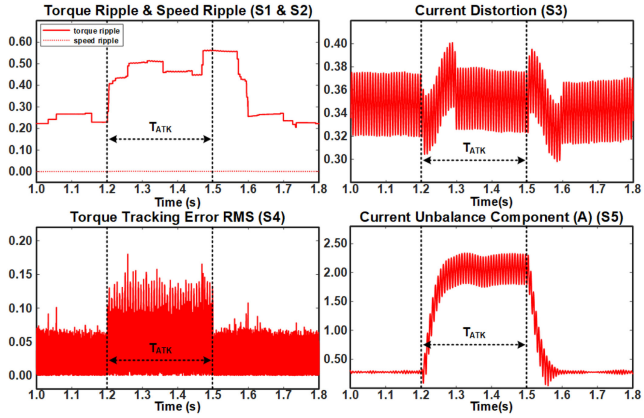


Fig. 9. Case 2: enlarging attacks, $\hat{y} = 1.2y,\ t \in \mathbf{T_{ATK}}$, targeting phase A.

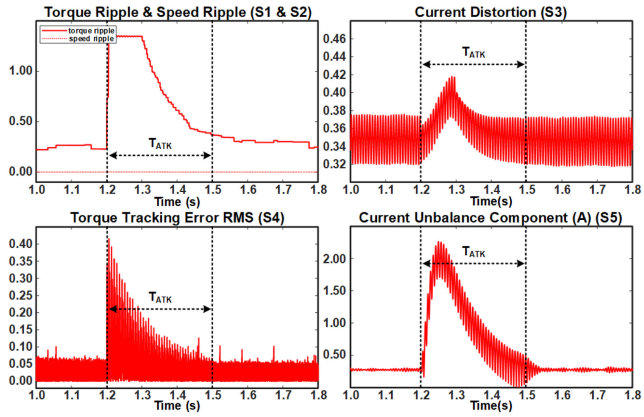


Fig. 10. Case 4: decaying high-frequency harmonics, $\hat{y} = y + 25e^{-t/0.1} \cdot \sin(2\pi \cdot 200 \cdot t),\ t \in \mathbf{T_{ATK}}$, targeting phase A.

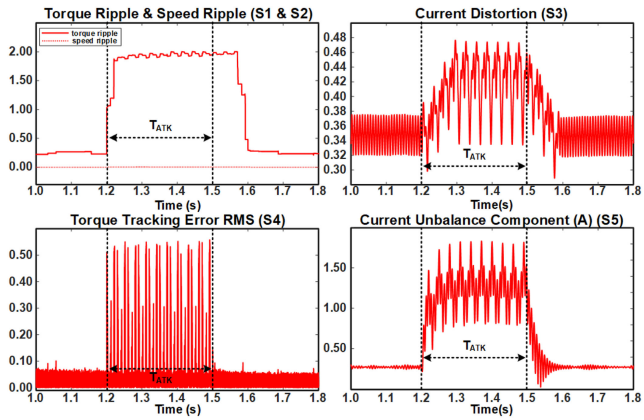


Fig. 11. Case 5: periodic pulse injection, $\hat{y} = y + \mathscr{F}(t),\ t \in \mathbf{T_{ATK}}$, targeting phase A.

1) Case 1. $\hat{y} = 0.8y,\ t \in \mathbf{T_{ATK}}$, Targeting Phase A: Fig. 8 shows the results when the feedback signal of phase A is reduced to 80% of the original value. It can be observed that this reduction can heavily deflect the actual current from its reference. Once the current of phase A increases, the current of phases B and C will drop to achieve the Kirchhoff current theorem. As a

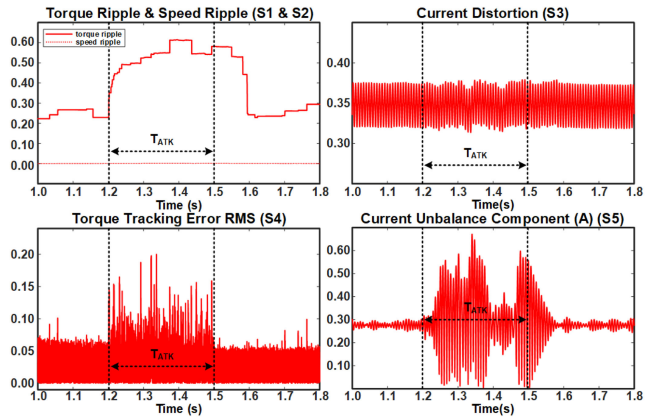


Fig. 12. Case 8: $\hat{y} = y +$ white noise, $t \in \mathbf{T_{ATK}}$, targeting phases A and B.

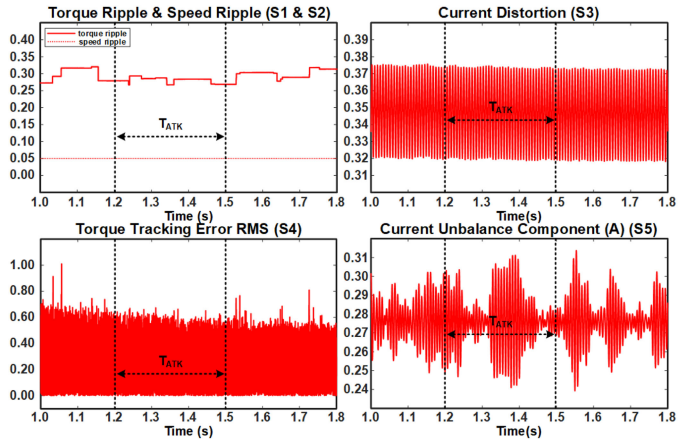


Fig. 13. Case 13: $\hat{y} = y +$ white noise, $t \in \mathbf{T_{ATK}}$, targeting phases A, B, and C.

consequence, the three phases become unbalanced, which is reflected by S_5 profile. Meanwhile, with the inaccuracy of the current value, torque ripple will be increased, and the current distortion will be worsened. It is also worth noting that all five metrics are bounded in the whole process, and when the attack is eliminated, the system performance could be restored, while a transient process is required.

2) Case 2. $\hat{y} = 1.2y$, $t \in \mathbf{T_{ATK}}$, Targeting Phase A: Fig. 9 shows the results when phase A current sensor signal is enlarged by 1.2 times. From the results, we can see that through the attack duration, the current of phase A decreases heavily, and that smaller current in phase A can lead to larger current in phases B and C. As the required torque cannot be provided in time, the torque controller intends to request larger current, which may cause the controller saturation, higher current distortion, tracking error, and ripples. Meanwhile, we notice that the changing pattern of the current distortion S_3 is opposite between cases 1 and 2, which could be a helpful tool to distinguish increasing attacks and decreasing attacks.

3) Case 4. $\hat{y} = y + 25e^{-t/0.1} \cdot \sin(2\pi \cdot 200 \cdot t)$, $t \in \mathbf{T_{ATK}}$, Targeting Phase A: Case 4 demonstrates the impact when a decaying high-frequency harmonics is introduced to phase A current feedback signals. The magnitude of the harmonics is 25 A, the decaying coefficient is 0.1, and the oscillation frequency is 200 Hz. The results are shown in Fig. 10. As shown in the figure, all metrics have a step change, and then, a decaying change similar to the attack appeals. This feature could be a useful tool for detecting and diagnosing the decaying attacks. However, it should be noted that some physical faults also have decaying characteristics, such as some short-circuit faults. So, in real applications, it should be addressed with enough attention for distinguishing physical faults and malicious attacks.

4) Case 5. $\hat{y} = y + \mathscr{F}(t)$, $t \in \mathbf{T_{ATK}}$, Targeting Phase A: Case 5 discusses the attack with a periodic pulse signal defined by (22), where $f = 1000$ Hz, $K = 30$ A, and $D = 0.25$. As shown by the results in Fig. 11, the system will have a periodic fluctuation with the similar frequency of the attack. Like Case 4, this feature could be used to determine if the attacks are periodic. From cases 4 and 5, it is obvious that when some false signals are injected to the sensor signals, the metric response will have a similar pattern to the injected signals. This could be used as one of the detection and diagnosis criteria.

5) Case 8. $\hat{y} = y +$ White Noise, $t \in \mathbf{T_{ATK}}$, Targeting Phases A and B: Case 8 talks about double-phase attack with white noise. Such attacks are rather more difficult to detect and diagnosis, because white noise is an inherent attribute for all sensors. It could easily trick people into wrong diagnostic conclusions, such as device aging or environment change. The results are shown in Fig. 12. When the same noise is injected to two phases (phases A and B), the three-phase current balance is damaged, but the current distortion is likely to maintain the healthy conditions as the noise power is relatively small. However, such small power noise is able to generate significant torque ripple. This case shows that not all evaluation metrics could reflect a deliberate designed attack, so the detection and diagnosis process needs to consider enough evaluation metrics to come up with the accurate conclusion.

6) Case 13. $\hat{y} = y +$ White Noise, $t \in \mathbf{T_{ATK}}$, Targeting Phases A, B, and C: When the noise is injected into all three sensors, the results of case 13 are shown in Fig. 13. It is hard to distinguish the attack duration from the metric waveform as the white noise power is relatively small. So, these kinds of attacks may not change the system operating conditions a lot. However, this also means that these kinds of attacks are hard to detect. In this case, the white noise could be brought by cyber-attacks like interception, where the system operation is not affected, but the system information is lost. Meanwhile, once the noise power becomes larger, it also could make the system unstable, as demonstrated in Section IV-A.

From the features of simulation results and the impact analysis of several typical cyber-attacks, a guideline for the sensor attack detection and diagnosis can be summarized as follows.

1) When one or more of the aforementioned performance metrics have drastic variation, there is likely an attack targeting on the system.
2) If the metric profiles maintain similar to the healthy operation conditions, it could be assumed that the system is not under attacks or the attack is minor and does not harm the system operating performance.

TABLE III
SIMULATION RESULTS OF ATK I

α	0.5	0.6	0.7	0.8	0.9
$\mathcal{K}_{imp}$	88.929	65.924	46.015	27.397	11.319
α	1.1	1.2	1.3	1.4	1.5
$\mathcal{K}_{imp}$	10.359	24.145	36.274	48.755	61.776

TABLE IV
SIMULATION RESULTS OF ATK II

β	-30	-20	-10	-5
$\mathcal{K}_{imp}$	82.839	52.774	24.773	11.090
β	5	10	20	30
$\mathcal{K}_{imp}$	10.931	24.460	53.273	84.070

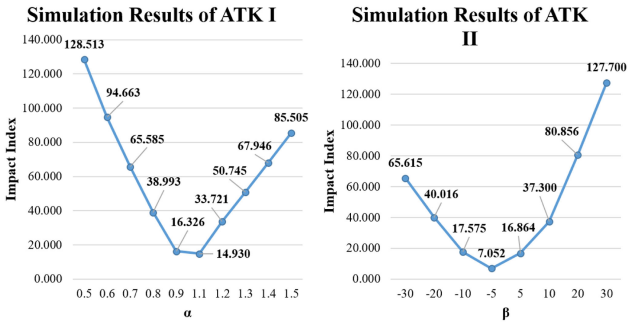


Fig. 14. Statistical diagram of Tables III and IV.

3) When the profile of the current distortion S_3 has two obvious spikes, there is likely an attack defined by (18). Then, its variation pattern could be used to determine if the attack increases or reduces the feedback signals.
4) If the current unbalance component (S_5) profile has a huge jump, it is likely a single-phase attack.
5) If the current unbalance component (S_5) is small or does not obviously change and other metrics (S_1–S_4) have abnormal profiles, it is likely a three-phase attack.
6) If the metrics have a decaying feature, the attack is likely to have the same decaying signal.
7) If the metrics have a periodic feature, the attack is likely an periodic signal with the same frequency.

C. Vulnerability Assessments of Different Attacks

In order to comprehensively assess the system vulnerability due to sensor data integrity attacks through the evaluation metrics and impact index we proposed, two types of common attacks modeled by (18) (ATK I) and (19) (ATK II) are simulated with $\alpha = 0.5, \ldots, 1.5$ and $\beta = -30, \ldots, 30$. The simulation results are shown in Tables III and IV, respectively.

From the results shown in Tables III and IV and Fig. 14, a ground truth could prove that the more deviation an attack could cause, the more severe impact it will bring to the systems. It should be noticed that the case where $\alpha < 0$ is not taking into consideration, because in such a case, the feedback control will become positive, which means that the system will be unstable,

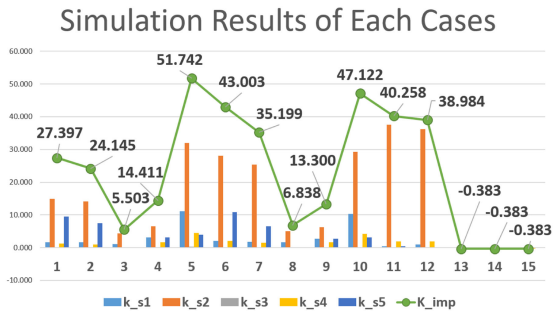


Fig. 15. Statistical graph of the simulation results.

and then, such attacks could be easily dealt with by protection components like relays.

Meanwhile, a statistical graph based on the results in Table II is shown in Fig. 15. In this diagram, each impact index is analyzed independently in each case. Then, we can make the following conclusions.

1) Three-phase attacks will barely have an impact on the electric drive system, as three-phase bias are filtered by DQZ transformation. Nevertheless, these kinds of attacks may also cause security issues from the other point of view, such as information stealing.
2) The impact of white noise attacks is relatively smaller, which means that such cyber-attacks are more difficult to detect. Besides, the impact of white noise is also dependent on the noise energy.
3) Except for three-phase additional attacks like cases 13–15, multiple phase attacks could cause more severe impact to the systems.
4) Among 15 cases we proposed, none of them has a drastic impact on $k_{\text{imp}}^{S_3}$, which means that these attacks will not drastically increase the current distortion. Thus, we could come to the conclusion that increasing current harmonic distortion requires more sophisticating attacks.

VI. CONCLUSION

This article presented a first systematic methodology to assess the vulnerability of electric drive systems due to sensor data integrity attacks. For demonstration purpose, an IPM-based electric drive system was modeled, and novel evaluation metrics from the perspectives of steady-state and transient performance were established to evaluate the system condition under different attacks. Then, a number of typical cyber-attacks were mathematically designed, and all evaluation metrics were calculated in a sliding window to generate time-series data of each cases. Based on the defined metrics and simulation results under 15 attack cases (five typical types), we proposed innovative index-based resilience and security criteria, together with the stability theorem, specifically for electric drive systems, which can then be used for cyber-attack detection and diagnosis in a more systematic manner. The qualitative attack impact on the dynamic characteristics and the statistical damage of different cyber-attacks were analyzed, which can serve as useful guidelines for attack detection, diagnosis, and countermeasures.

REFERENCES

[1] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Syst. Mag.*, vol. 35, no. 1, pp. 110–127, Feb. 2015.

[2] F. Li, Y. Shi, A. Shinde, J. Ye, and W.-Z. Song, "Enhanced cyber-physical security in Internet of Things through energy auditing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5224–5231, Jun. 2019.

[3] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, and W.-Z. Song, "System statistics learning-based IoT security: Feasibility and suitability," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6396–6403, Aug. 2019.

[4] U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and recommendations," U.S. Dept. Energy, Washington, DC, USA, Tech. Rep. CA0401194, Apr. 2004.

[5] S. Cherry and R. Langner, "How Stuxnet is rewriting the cyberterrorism playbook," *Computerworld*, 2010. [Online]. Available: https://spectrum.ieee.org/podcast/telecom/security/how-stuxnet-is-rewriting-the-cyberterrorismplaybook, Accessed: Oct. 13, 2010.

[6] R. McMillan, "Siemens: Stuxnet worm hit industrial systems," *Computerworld*, vol. 14, 2010. [Online]. Available: https://www.computerworld.com/article/2515570/siemens--stuxnet-worm-hit-industrial-systems.html, Accessed: Sep. 14, 2010.

[7] K. Zetter, "A cyberattack has caused confirmed physical damage for the second time ever," 2015.

[8] *Experimental Security Research of Tesla Autopilot*, Tencent Keen Security Lab, 2019.

[9] I. Ilascu, "HVACking: Remotely exploiting bugs in building control systems." [Online]. Available: https://www.bleepingcomputer.com/news/security/hvacking-remotely-exploiting-bugs-in-building-control-systems/, Accessed: Aug. 13, 2019.

[10] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *Proc. IEEE PES Gen. Meeting*, Jul. 2010, pp. 1–6.

[11] L. R. Phillips *et al.*, "Analysis of operations and cyber security policies for a system of cooperating flexible alternating current transmission system (FACTS) devices," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2005-7301, 2005.

[12] R. Berthier, W. H. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 350–355.

[13] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1052–1062, May 2013.

[14] A. Subasi *et al.*, "Intrusion detection in smart grid using data mining techniques," in *Proc. 21st Saudi Comput. Soc. Nat. Comput. Conf.*, Apr. 2018, pp. 1–6.

[15] L. Zhou, X. Ouyang, H. Ying, L. Han, Y. Cheng, and T. Zhang, "Cyber-attack classification in smart grid via deep neural network," in *Proc. 2nd Int. Conf. Comput. Sci. Appl. Eng.*, 2018, Art. no. 90.

[16] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.

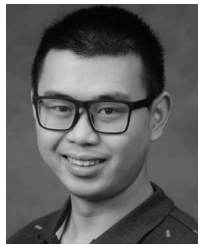
[17] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," in *Proc. Amer. Control Conf.*, Jun. 2010, pp. 962–967.

[18] C. Ten, G. Manimaran, and C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

[19] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response," in *Proc. 6th ACM Symp. Inf., Comput. Commun. Secur.*, 2011, pp. 355–366.

[20] I. Kiss, B. Genge, and P. Haller, "A clustering-based approach to detect cyber attacks in process control systems," in *Proc. IEEE 13th Int. Conf. Ind. Informat.*, 2015, pp. 142–148.

[21] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, and S. Sastry, "Understanding the physical and economic consequences of attacks on control systems," *Int. J. Crit. Infrastructure Protection*, vol. 2, no. 3, pp. 73–83, 2009.



Bowen Yang received the B.S. degree in electrical engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2018. He is currently working toward the Ph.D. degree electrical and computer engineering with the University of Georgia, Athens, GA, USA.

He is currently a Research Assistant with the University of Georgia. His current research interests include advanced control for power electronics and electric machines, energy management systems, and cyber-physical security for intelligent electric drives.

Lulu Guo received the B.S. degree in vehicle engineering and the Ph.D. degree in control engineering from Jilin University, Changchun, China, in 2014 and 2019, respectively.

He is currently a Postdoctoral Research Associate with the University of Georgia, Athens, GA, USA. His current research interests include advanced vehicle control, energy management, and vehicle cybersecurity.

Fangyu Li received the B.S. degree from Beihang University, Beijing, China, in 2009, and the M.S. degree from Tsinghua University, Beijing, in 2013, both in electrical engineering, and the Ph.D. degree in geophysics from the University of Oklahoma, Norman, OK, USA, in 2017.

He is currently a Postdoctoral Fellow with the College of Engineering, University of Georgia, Athens, GA, USA. His current research interests include signal processing, seismic imaging, machine learning, deep learning, distributed computing, Internet of Things, and cyber-physical systems.

Jin Ye (S'13–M'14–SM'16) received the B.S. and M.S. degrees from Xi'an Jiaotong University, Xi'an, China, in 2008 and 2011, respectively, and the Ph.D. degree from McMaster University, Hamilton, ON, Canada, in 2014, all in electrical engineering.

She is currently an Assistant Professor of Electrical Engineering and the Director of the Intelligent Power Electronics and Electric Machines Laboratory, University of Georgia, Athens, GA, USA. Her current research interests include power electronics, electric machines, energy management systems, smart grids, electrified transportation, and cyber-physical systems.

Dr. Ye is the General Chair of the 2019 IEEE Transportation Electrification Conference and Expo and the Publication Chair and Women in Engineering Chair of 2019 IEEE Energy Conversion Congress and Expo. She is an Associate Editor for the IEEE TRANSACTIONS ON TRANSPORTATION ELECTRIFICATION and the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.

Wenzhan Song received the B.S. and M.S. degrees from the Nanjing University of Science and Technology, Nanjing, China, in 1997 and 1999, respectively, and the Ph.D. degree in computer science from the Illinois Institute of Technology, Chicago, IL, USA, in 2005.

He is currently the Chair Professor of Electrical and Computer Engineering with the University of Georgia, Athens, GA, USA. His current research interests include cyber-physical systems and their applications in energy, environment, food, and health sectors.

Dr. Song received the National Science Foundation CAREER Award in 2010.