Resilient Cyber-Physical Power Protection Systems Using Transient Kinetic Energy Method

Seyed Hossein Rouhani, *Member, IEEE*, Chun-Lien Su, *Senior Member, IEEE*, Hamid Reza Shabani, Mostafa Esmaeili Shayan, Saleh Mobayen, *Senior Member, IEEE*, Navid Razmjooy, *Senior Member, IEEE*, Jin-Ting Yu, *Student Member, IEEE*, and Chih-Yuan Chiang

***Abstract*—The integration of remote control and digitalization in intelligent power systems has introduced significant cybersecurity risks, particularly from malicious attacks targeting protection systems, which can lead to operational disruptions and line outages. However, such outages may also arise from system faults, protection failures, or circuit breaker malfunctions. To address this challenge, this article introduces a novel methodology based on waveform analysis. The proposed approach leverages transient kinetic energy analysis and real-time circuit breaker monitoring to differentiate between cyber-attacks and other causes of line outages. By analyzing waveform data from circuit breaker (CB) coil current and contact travel, the method extracts timing features to assess CB health. Probability distribution curves are generated for each feature, enabling new measurements to be compared within these distributions to evaluate CB conditions. Numerical simulations on a modified IEEE 39-bus test system, supported by experimental tests, reveal a key finding: during power system faults, a distinct time delay occurs between abrupt changes in transient kinetic energy and the initiation of line outages. In contrast, this delay is absent in cases of cyber-attacks and circuit breaker failures. This innovative method can be seamlessly integrated into supervisory control and data acquisition systems, enabling real-time identification of the root causes of outages and significantly enhancing the cybersecurity of power systems.**

***Index Terms*—Circuit breaker failure detection, false command cyber-attack detection, time domain simulation, transient kinetic energy, waveform analysis.**

Received 10 October 2024; revised 5 January 2025; accepted 10 April 2025. This work was supported in part by the National Science and Technology Council of Taiwan under Grant NSTC 111-2923-E-992 -001-MY3, Grant NSTC 113-2221-E-992-037, and Grant NSTC 113-2218-E-992-003. Paper no. TII-24-5320. *(Corresponding author: Chun-Lien Su.)*

Seyed Hossein Rouhani, Chun-Lien Su, Jin-Ting Yu, and Chih-Yuan Chiang are with the Department of Electrical Engineering, National Kaohsiung, University of Science and Technology, Kaohsiung 807618, Taiwan (e-mail: hosseinrouhani@nkust.edu.tw; cls@nkust.edu.tw; i109154103@nkust.edu.tw; i110154107@nkust.edu.tw).

Hamid Reza Shabani is with the Center of Excellence for Power System, Automation and Operation, Department of Electrical Engineering, Iran University of Science and Technology, Tehran 1684613114, Iran (e-mail: h_shabani@alumni.iust.ac.ir).

Mostafa Esmaeili Shayan is with the Department of Mechanical, Chemical and Materials Engineering, University of Cagliari, 09123 Cagliari, Italy (e-mail: mostafa.esmaeili@unica.it).

Saleh Mobayen is with the Graduate School of Intelligent Data Science, National Yunlin University of Science and Technology,, Douliou 640301, Taiwan (e-mail: mobayens@yuntech.edu.tw).

Navid Razmjooy is with the Department of Computer Science and Engineering, Division of Research and Innovation, Saveetha School of Engineering, SIMATS, Chennai 602105, India (e-mail: xnavid@gmail.com).

Digital Object Identifier 10.1109/TII.2025.3563547

Nomenclature

SCADA	Supervisory control and data acquisition.
RTUs	Remote terminal units.
CB	Circuit breaker.
TKE	Transient kinetic energy.
CT	Current transformer.
PT	Potential transformer.
SV	Sampled values.
MMS	Manufacturing message specification.
GOOSE	Generic object-oriented substation event.
DFIG	Doubly fed induction generators.
SF6	Sulfur hexafluoride.
HIL	Hardware-in-the-loop.
T-D	Time-domain.
RBFN	Radial basis function network.

I. Introduction

PROTECTION systems play a vital role in power systems characterized by a significant presence of renewable energy generating sources and bidirectional power flow. These systems are designed to safeguard power systems from potential defects and disruptions. The purpose of this system is to autonomously identify and isolate errors. In addition to the autonomous feature and in conjunction with safeguarding concerns, operators within the SCADA facility employ RTUs to assess the status of the power system. Subsequently, operators issue commands to protection relays based on the system's condition, initiating the disconnection of a power line. Although power system protection engineers hold the belief that a simpler protective system offers greater reliability, the integration of intelligent electrical embedded devices with the new generation of protection relays in smart power systems has enhanced the protection of smart renewable power systems.

Distance relays are utilized to protect high-voltage transmission lines by employing impedance estimation techniques that rely on measured current and voltage data. The predicted impedance is afterward compared to the impedance of the protected zone. If the estimated impedance exceeds the zone impedance, the relay sends a trip command to the CB. However, under specific fault conditions such as voltage instability, power fluctuations, or load invasion, distance relays may face

challenges in accurately measuring the impedance of zone three [1], leading to the issue of false trip commands. In addition, false commands issued by malicious assaults also lead to false trips. On the other hand, from the perspective of protection engineering, it is highly unlikely for a CB to experience an open without commands failure due to the presence of a lock mechanism that keeps it in either the open or closed position during internal fault conditions. However, according to the findings of the CIGRE working group, the failure rate for an open without commands failure is reported to be 5.4%. This failure rate is primarily attributed to internal failures within the CB [2].

The operational state of each CB inside the SCADA system is continuously monitored and visually represented as either activated (ON), deactivated (OFF), or experiencing a malfunction (failure). The failure status is characterized by the absence of faults during operation or the failure to operate following a fault and remote instruction. The SCADA system lacks an additional algorithm for identifying the cause of its failure. In order to detect early CB failure, online monitoring has been proposed [2], [3], where the CB condition is evaluated by the operation time of the electrical and mechanical parts. In [4], a novel CB fault detection method based on online monitoring has been proposed, considering that the industry leaders in this field have actively developed and implemented online CB monitoring capabilities. In [5], the researchers have presented a proposed methodology for the prediction of circuit breaker failure by utilizing vibration measurement data obtained during switching operations.

The advent of digitization and remote access has rendered protection systems vulnerable to cyber-attacks [6], [7]. Cyber attackers attempt to manipulate the internal settings of protection systems, like critical clearing time and thresholds for zone settings, or to falsify the SCADA commands and send fake trip signals to CBs through remote access, resulting in line outages [8]. Outages can lead to the overloading of other lines within the system, reducing the stability margin, which can consequently lead to transient instability and cascading failures [9]. According to Hong et al. [7], cyber-attacks targeting distance relay settings can be prevented by establishing communication between neighboring relays. Distance relays are distributed all over the transmission system and overlap to provide comprehensive protection. Considering this, a multiagent-based deep learning method is presented in [10] for detecting cyber-attacks. This method involves comparing the measured local voltage and current with neighboring relays. In practical terms, the implementation of this method requires comprehensive and accurate information from all the relays involved, increasing the complexity and challenges of the process. The ability of the data mining methods to detect disturbances, normal control operations, and cyber-attacks targeting protection systems has been demonstrated in [11], which necessitates comprehensive and accurate historical information to effectively analyze the current condition of the system. The sliding mode control approach, as developed in [12], has been used for online cyber-attack detection. However, this method heavily relies on the precise modeling of the system. In [13], a secure sampled measured value message has been proposed to secure the transmitted data regarding communication delays. However, this method has practically proven to secure digital substation communications. However, the vulnerability persists in the face of cyber-attacks targeting internal settings changes in protection systems, CT and PT tap changers, and direct commands originating from the SCADA system. In [14], the cyber-attack detection index has been developed based on wavelet analysis of the current signal. In [15], the authors propose a blockchain-assisted, fully distributed identity-based digital signature scheme that eliminates the need for a trusted Key Generation Center, improves efficiency using oblivious transfer, and ensures existential unforgeability. In [16], a combination of an optimized homomorphic convolutional neural network and a lightweight threshold signature scheme-based dual-authorization protocol is proposed to enhance data security. A random forest decision machine learning algorithm has been developed in [17] to detect and mitigate cyber-attacks against the protection systems. To overcome these methods, attackers are constantly attempting to design new types of cyber-attacks, called stealthy cyber-attacks, which remain undetected by security systems [18], [19]. In [20], an unknown input observer has been proposed for detecting stealthy attacks. In [21], a method based on the Shewhart test and the sliding-window chi-squared test has been developed to address stealthy cyber-attacks. Data-driven detection [22], a switching multiplicative watermarking strategy [23], and a permutation entropy-based method [22] are some methods against stealthy cyber-attacks. Despite their advantages, the mentioned methods have limitations, including a tendency to require significant amounts of time, inherent complexity, questionable efficacy in online detection scenarios, vulnerability to new stealthy cyber-attacks, and reliance on specific system models.

To address the drawbacks of previously developed methods, this work presents a strategy for detecting stealthy cyber-attacks by considering the behavior of the power system's transient kinetic energy during system operations and online monitoring of the CBs. The proposed method is practical. This strategy utilizes waveform data from the coil current and contact travel of CBs to extract timing features for assessing their health conditions. Probability distribution curves are then generated for each timing feature, allowing for the evaluation of CB health based on new measurements within these distributions. On the other hand, it also utilizes the TKE behavior in power systems. The TKE exhibits a direct proportionality to the square of the velocity differential between the reference generator and the remaining generators. The TKE experiences a sudden large increase in magnitude at the occurrence of a fault, followed by a subsequent drop upon the resolution of the fault. If the system achieves stability after the fault has been removed, the TKE will tend towards a value close to zero. Nevertheless, in the event that the system continues to exhibit instability, there will be a resurgence in TKE [24].

The proposed method is based on considering the correlation between TKE and the loss of power system synchronization during a fault and online CB monitoring. The rationale underlying the utilization of the proposed methodology is related to two factors: first, acknowledging that industry leaders are developing online monitoring of CBs, and second, the SCADA system currently monitors the velocity of the generators and their rates of change by RTUs. Therefore, the proposed method can be integrated into existing SCADA algorithms. The main contributions of this research article can be summarized as follows.

1) Developing a novel waveform-based method for real-time detection of line outage reasons while meticulously accounting for real-world practical limitations.
2) The developed method doesn't need the system model, relying solely on data from circuit breaker monitoring and synchronism generator speed provided by RTUs.

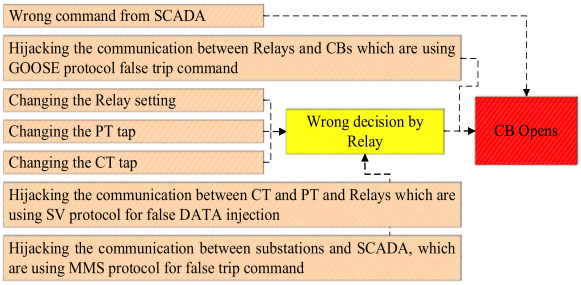

Fig. 1. Cyber-attack tree for protection systems.

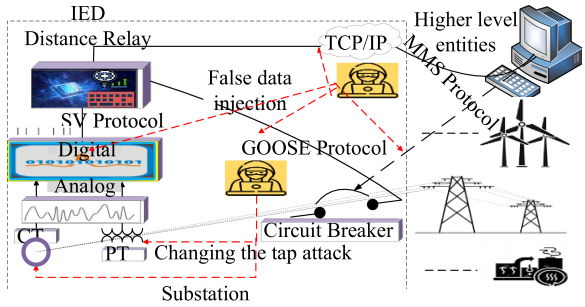

Fig. 2. Schematic of the communication protocol in a smart power system.

3) The proposed method is robust against stealthy cyber-attacks.

The rest of this article is structured in the following manner. The studied power system modeling for TKE monitoring and the evaluation of circuit breaker health conditions are explicitly outlined in Section II. Section III discusses the proposed transient kinetic energy monitoring and circuit breaker health condition monitoring methods. The innovative approach includes extracting time features to identify healthy conditions and utilizing TKE variations to discern faults and malfunctions in power systems. Section IV contains a discussion of practical considerations. The findings and analysis of the test results are reported in Section V. Section VI concludes this article.

II. Problem Formulation

The cyber-attack tree for the problem considered in this paper is illustrated in Fig. 1. As illustrated in this figure, attackers employ various sophisticated techniques to replace accurate data with false or manipulated information.

These attacks target not only critical communication channels and data exchange systems but also measurement sensors. This manipulation results in the maloperation of protection devices, leading to false trips, which can undermine the stability and security of the power system. Given the nature of these attacks, they fall under the category of false data injection cyber-attacks.

Among the mentioned possible cyber-attacks on the protection system, a communication-based technique between neighboring distance relays can prevent cyber-attacks that change protection distance relay settings [7]. This strategy is possible because smart power system substations and control centers are strongly connected. Thus, false data injections and commands are their biggest vulnerabilities. Furthermore, the occurrence of protection system malfunctions introduces the possibility of false tripping. Several circumstances cause these malfunctions, which area as follows.

1) CTs and PTs maloperation, saturations, Ferro-resonance phenomena, and their internal defects.
2) Distance relays zone three maloperation and their internal defects.
3) The internal defects of the CBs.

Under saturation conditions, distance relays experience a reduced effective current, leading to a higher calculated impedance and inducing a time delay in relay operation [25], [26]. As a result, this event cannot affect the CB open without command failure. On the other hand, in the Ferro-resonance phenomenon, the magnitude of voltage and current increases, leading to the overreaching of distance relays and, consequently, false trip commands due to lower impedance estimation [27], [28]. To eliminate this kind of maloperation, researchers have proposed applicable methods [29], [30]. Digital relays are equipped with various detection methods and prevention filters [31], making the current technology less susceptible to this type of maloperation. Among the mentioned factors, critical events involve malfunctions in the three distance relay zones and circuit CBs internal faults. Therefore, other factors are beyond the scope of this study. Fig. 2 illustrates how attackers perform malicious activities against the issues described in this study.

As illustrated in Fig. 2, the SCADA system, considering the power system status, transmits new reference points and commands to the substations through the communication infrastructure, utilizing the MMS protocol. Within substations, intelligent electronic devices receive measurements from CTs and PTs through communication channels using SV protocols. Based on these measurements, relays send instructions to CBs via the GOOSE protocol. Cyber attackers exploit vulnerabilities by gaining remote or physical access to control centers and substations. They may also intercept communication between the control system and substations, including internal substation communication. Through these means, attackers manipulate measured or transmitted data, inserting false information or sending deceptive commands to disrupt the actions of protection systems. To detect these kinds of cyber-attacks, this article proposes a model-free-based waveform analysis considering real-world applications. The proposed strategy utilizes real-time monitoring data from healthy condition monitoring of CB and synchronism generator speed provided by RTUs. While the proposed method does not require system modeling, for an effective demonstration of its performance, we initially utilize an accurate model to mimic the real-world behavior of renewable power systems and monitor TKE. Additionally, we introduce a novel, robust approach for evaluating the status of circuit breakers through online monitoring. In practical implementation, only the mentioned data will be used, eliminating the need for the exact modeling of the system.

A. System Model for Transient Kinetic Energy

Consider a multi-machine dynamic system with a set of differential and algebraic equations:

$$\dot{x} = f(x, z, u) \tag{1}$$

$$0 = g(x, z, u) \tag{2}$$

where x represents the system states, u indicates the system inputs, $f(.)$ represents the system differential equations, and $g(.)$

indicates the system governing algebraic equations. Although a classical model of the reduced power system to internal generator nodes may have acceptable accuracy for using the transient energy methods [32], this article takes a step further by considering and developing a two-axis model of synchronous generators (SGs) with a static excitation system, incorporating the penetration of wind power to enhance accuracy. The renewable power system under consideration involves *m* machines and is described by the following two-axis model [33]:

$$T_{d0i}^{'}\frac{d}{dt}E_{qi}^{'} = -E_{qi}^{'} - \left(X_{di} - X_{di}^{'}\right) I_{di} + E_{fdi} \tag{3}$$

$$T_{q0i}^{'}\frac{d}{dt}E_{di}^{'} = -E_{di}^{'} + \left(X_{qi} - X_{qi}^{'}\right) I_{qi} \tag{4}$$

$$\frac{d}{dt}\delta_i = \omega_i - \omega_s \tag{5}$$

$$M_i\frac{d}{dt}\omega_i = T_{Mi} - T_{Ei} - D_i\left(\omega_i - \omega_s\right) = f_i\ (\delta) \tag{6}$$

$$\boldsymbol{s}T_{Ai}\frac{d}{dt}E_{fdi} = -E_{fdi} + K_{Ai}\left(V_{\text{ref}i} - V_{ti}\right) \tag{7}$$

$$T_{Ei} = \left[E_{di}^{'}I_{di} + E_{qi}^{'}I_{qi} + \left(X_{qi}^{'} - X_{di}^{'}\right) I_{di}I_{qi}\right] \tag{8}$$

and

$$E_{di}^{'} - V_{ti}\sin\left(\delta_i - \theta_{ti}\right) - R_{si}I_{di} + X_{qi}^{'}\,I_{qi} = 0 \tag{9}$$

$$E_{qi}^{'} - V_{ti}\cos\left(\delta_i - \theta_{ti}\right) - R_{si}I_{qi} - X_{di}^{'}\,I_{di} = 0 \tag{10}$$

where $i = 1, 2, \ldots, m$ is the number of the generator. $T_{d0i}^{\prime}$, $E_{di}^{\prime}$, X_{di}, $X_{di}^{\prime}$, I_{di}, and E_{fdi} are open circuit time constant, transient voltage of SG, synchronous, and transient reactance, current, and field winding voltage, respectively, all for *d*-axis. $T_{q0i}^{\prime}$, $E_{qi}^{\prime}$, X_{qi}, $X_{qi}^{\prime}$, and I_{qi} are open circuit time constant, transient voltage of SG, synchronous, and transient reactance, and current, respectively, all for *q*-axis. T_{Mi}, and $T_{Ei}$are mechanical and electromagnetic torque. V_{ti}, and $V_{\text{ref}i}$ are terminal and excitation reference voltage. δ_i, and θ_{ti} are rotor and terminal voltage angle. R_{si}, K_{Ai}, ω_i, ω_s, M_i, D_i, and T_{Ai} are blade length, excitation gain, rotor velocity, synchronous speed, inertia, and damping constant, respectively.

For the wind power generation model, DFIGs are considered. The drive-train system, induction generator, and power electronics converters are parts of the DFIG. In this manner, each component of the DFIG is separately modeled. Although the wind turbine aerodynamic system is typically represented by an algebraic model, its mechanical dynamics are disregarded for stability studies [34]. In a wind turbine, the extracted power can be calculated by the following:

$$P_{tw} = (0.5)\,\rho\pi R^2 C_p\left(\lambda, \beta\right) V_w^3 \tag{11}$$

where C_p, λ, β, and V_w are wind turbine performance coefficient, tip speed ratio, blade pitch angle, and wind speed, respectively. ρ represents air density, and R is blade length. The λ can be obtained by

$$\lambda = \left(\omega_t.R\right)/V_w \tag{12}$$

where ω_t is the wind turbine speed. While analyzing the stability of the wind turbine drive-train system, experimental investigations and power system simulations recommend the use of a two-mass model [35], [36] that is used for modeling DFIG. Typically, the dynamic analysis of the power system does not consider the stator transients in asynchronous and SGs. Hence, in the transient stability simulation algorithms [36], the currents and voltages are represented as phasors. Since the stator transients are likewise disregarded in this study, the induction generator dynamic equations are stated as follows [37], [38]:

$$V_{qs} = -r_s\,i_{qs} + e_q^{'} - L_s^{'}i_{ds} \tag{13}$$

$$V_{ds} = -r_s\,i_{ds} + e_d^{'} + L_s^{'}i_{qs} \tag{14}$$

$$V_{qs} = -r_s\,i_{qs} + e_q^{'} - L_s^{'}i_{ds} \tag{15}$$

$$V_{ds} = -r_s\,i_{ds} + e_d^{'} + L_s^{'}i_{qs} \tag{16}$$

$$T_e = e_d^{'}i_{ds} + e_q^{'}i_{qs} \tag{17}$$

and

$$\frac{1}{\omega_b}\frac{d}{dt}e_d^{'} = \frac{1}{T_0}\left(-e_d^{'} + \left(L_{ss} - L_s^{'}\right) i_{qs}\right) + \left(1 - \omega_r\right) e_q^{'} - \frac{L_m}{L_{rr}}V_{qr} \tag{18}$$

$$s\frac{1}{\omega_b}\frac{d}{dt}e_q^{'} = -\frac{1}{T_0}\left(e_q^{'} + \left(L_{ss} - L_s^{'}\right) i_{ds}\right) - \left(1 - \omega_r\right) e_d^{\prime} + \frac{L_m}{L_{rr}}V_{dr} \tag{19}$$

where i_{qs}, V_{qs}, $e_q^{\prime}$, i_{ds}, V_{ds}, $e_d^{\prime}$, and V_{qr} are current, stator and internal voltage in *q* and *d* axis and rotor voltage of the doubly fed induction generator, respectively. The parameters r_s, and r_r are stator and rotor resistance, respectively. L_{ss}, L_{rr}, and L_m are stator, rotor, mutual inductance of the doubly fed induction generator, respectively. T_e is of wind turbine electrical torque. The terms T_0, $e_d^{\prime}$, $L_s^{\prime}$, and $e_q^{\prime}$ are equal with

$$e_d^{'} = -\frac{L_m}{L_{rr}}\lambda_{qr} \tag{20}$$

$$T_0 = \frac{L_{rr}}{r_r} \tag{21}$$

$$L_s^{'} = \left(L_{ss} - \frac{L_m^2}{L_{rr}}\right) \tag{22}$$

$$e_q^{'} = \frac{L_m}{L_{rr}}\,\lambda_{dr}. \tag{23}$$

The nonlinear algebraic current-balance equations for power systems with synchronism and DFIG are shown as follows:

$$\left(I_{di} + jI_{qi}\right) e^{j\left(\delta_i - \frac{\pi}{2}\right)} = \sum_{i=1}^{m}\left[\left(Y_{ik}^{\prime}e^{j\alpha_{jk}^{\prime}}\right)\left(V_{tk}e^{j\theta_{tk}}\right)\right]. \tag{24}$$

For doubly fed induction generator V_t is defined as follows:

$$V_{td}\,e^{j\theta_{td}} = \left[V_{ds} + jV_{qs}\right]\,e^{j\left(\delta - \frac{\pi}{2}\right)}. \tag{25}$$

In a doubly fed induction generator, the terminal voltage vector is synchronized with the q-axis. Therefore

$$V_{ds} = 0 \rightarrow \begin{cases} V_{td} = V_{qs} \\ \theta_{td} = \delta \end{cases}. \tag{26}$$

The grid side converter is defined with a current source, and reactive power is exchanged with the power system by stator. Thus, the grid-side converter is modeled as follows:

$$I_{\text{Grid side conv}} = \frac{P_{\text{Grid side conv}} - Q_{\text{Grid side conv}}}{-jV_{qs}}. \tag{27}$$

Finally, the injected current by doubly fed induction generator is shown as follows:

$$\left(I_{dtd}+jI_{qtd}\right)e^{j\left(\theta_{td}-\frac{\pi}{2}\right)}=\sum_{i=1}^{m}\left[\left(Y'_{ik}e^{j\alpha'_{jk}}\right)\left(V_{tk}e^{j\theta_{tk}}\right)\right]. \tag{28}$$

After simultaneously solving the differential and algebraic equations of the modeled system, the rotor speed and angle are calculated. Unlike the classical model, in this study, it is not necessary to transfer them to the center of inertia, and the generator is taken as a reference. The TKE function can be evaluated by considering the difference between the generator speed and reference, as follows [32]:

$$V_{KE}=\sum_{i=1}^{m}\frac{1}{2}M_i(\omega_i-\omega_s)^2. \tag{29}$$

In the real-world application of the proposed method, one only needs to gather information from the RTUs and monitor the TKE, as specified in (29).

B. Circuit Breaker Failure Evaluation

The SCADA system continuously monitors the status of high-voltage transmission CBs, effectively discerning three distinct states: ON, OFF, and Failure. A CB is identified as a failure when it fails to operate following a fault or a remote order**.** The current SCADA system lacks adequate supplementary measures for determining the root cause of failures. On the other hand, industry leaders are actively developing real-time monitoring capabilities for CBs. In light of this situation, the objective of this study is to address the SCADA deficiency by leveraging real-time monitoring data from CBs for early failure detection**.** This novel approach will facilitate the distinction between CB failures, power system faults, and cyber-attacks. CBs consist of two primary components, namely, the control section and the operational section. The CB structure incorporates a hydraulic spring that functions to store energy when the contacts are in a closed state. To activate a CB, the trip coil must be supplied with electrical energy, derived from the trip battery. To ascertain instances of failure, it is imperative to conduct a comprehensive examination of both the control and operational components, along with their respective subcomponents.

The causes of control circuit breaker failures are frequently attributed to various factors, including wiring errors (such as incorrect connections), short circuits, external interference (such as electromagnetic interference and electrical noise), environmental conditions (such as extreme temperatures, humidity, dust, and corrosive substances), and vibration, mechanical stress, aging, and deterioration. Furthermore, various occurrences such as the failure of the trip mechanism, spring failure, misalignment or binding in the moving parts, malfunction of the latch or locking mechanism, and manufacturing defects can be considered instances of potential malfunctions in the mechanical components of circuit breakers. These malfunctions can cause circuit breaker openings without external commands.

As reported in papers [2] and [39], the data from real-time monitoring can be used to detect high-voltage CB failure early. Through the analysis of the waveforms using signal processing methods, the functional features can be extracted. However, as shown in [2], the timing features (t_1 to t_4) mentioned in Table I provide adequate accuracy for early failure detection. Additionally, we propose using the contact travel time (t_5) to detect mechanical failure. Fig. 3 shows the coil current and contact travel waveform during CB open operation.

TABLE I
TIMING SELECTED FEATURES FROM CB ONLINE MONITORING

Events	Times
Trip operation is started	t_1
Trip coil current picks up	t_2
Trip coil current dips after saturation	t_3
Trip coil current drops off	t_4
Contact breaks or makes (a change of status from low to high or vice versa) travel time	t_5

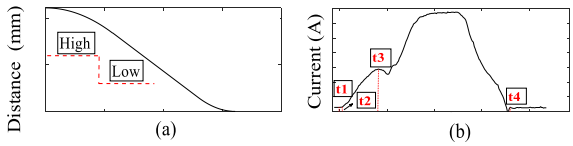

Fig. 3. CB trip operation. (a) Contact travel waveform. (b) Coil current.

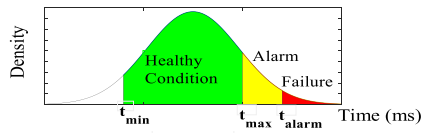

Fig. 4. Probability distribution for CB monitoring.

The performance of CBs in high-voltage transmission systems is affected not only by timing parameters but also by critical factors related to the SF6 gas, which is used as an insulating medium. Moisture, pressure, purity, leakage, and SF6 gas are essential considerations. Adhering to the manufacturer-defined limits for these characteristics is crucial for proper CB operation during opening or closing actions. Exceeding these limits can lead to decreased insulating properties, impacting CBs during arc phenomena and potentially preventing proper opening due to reduced insulating properties and electric arc extinguishing capability. Failures related to SF6 gas properties must be thoroughly investigated, especially when the CB is in the open position. For example, increased moisture content can cause flashover when the CB is opened. Regular monitoring and maintenance of SF6 gas properties is essential to ensure the reliable and safe performance of CBs in high-voltage transmission systems [40]. By utilizing online monitoring, the operator will have sufficient data to compose an accurate probability distribution for each timing feature. An example of a probability distribution for CB monitoring is shown in Fig. 4. Over the course of time, the timing features of circuit breakers which have been extracted and updated over time may gradually shift towards alert areas due to aging and the effects of friction. Nevertheless, through appropriate maintenance practices, it is possible to restore them to an optimal health condition.

The evaluation of the probability of the circuit breakers being in a healthy state can be performed by the following:

$$P_{t_i}^{\text{Healthy}}=\int_{t_{\min}}^{t_{\max}} f_{t_i}\,dt \tag{30}$$

$$P_{t_i}^{\text{Alarm}}=\int_{t_{\max}}^{t_{\text{alarm}}} f_{t_i}\,dt \tag{31}$$

$$P_{t_i}^{\text{Failure}} = 1 - \sum \left(P_{t_i}^{\text{Healthy}}, P_{t_i}^{\text{Alarm}} \right) \tag{32}$$

$$f_{t_i} = \frac{1}{\partial\sqrt{2\pi}} e^{\frac{-(t_i-\mu)^2}{2\partial^2}} \tag{33}$$

where $P_{t_i}^{\text{Healthy}}$, $P_{t_i}^{\text{Alarm}}$, f_{t_i}, ∂, and μ are CB healthy condition probability, CB alarm condition probability, probability distribution, standard deviation, and mean, respectively. Since this article focuses on failures that occur when the circuit breaker opens without commands, the probability of such failures will be discussed in the following sections. To this end, two factors, including the trip coil current signal and traveling contacts performance, are investigated. The performance probability for trip coil current is defined as follows:

$$HP_{\text{Trip coil}}^{\text{Failure}} = 1 - \prod_{i=2}^{4} P_{t_i}^{\text{Failure}}. \tag{34}$$

Traveling contacts performance in CB acts properly if the timing "t_5" is within its correct interval. The mechanical part performance probability is defined as follows:

$$HP_{\text{Contacts travel}}^{\text{Failure}} = 1 - P_{t_5}^{\text{Failure}}. \tag{35}$$

In summary, the probability of the CB performance is evaluated by the following:

$$HP_{CB}^{\text{Failure}} = 1 - \prod_{i=2}^{5} P_{t_i}^{\text{Failure}}. \tag{36}$$

III. Proposed Method

To discern the causes of line outages, including malicious cyber activities, power system faults, or protection system malfunctions, this article introduces a novel waveform analysis method. The motivation for differentiating between faults and cyber-attacks in this research stems from their potential to cause similar disruptions, such as line outages, despite differing in frequency and nature. Faults typically result from natural causes, while cyber-attacks can deliberately mimic these events. Accurate differentiation ensures appropriate, timely responses, avoiding unnecessary interventions like maintenance for cyber-attacks. Although digital logs can identify cyber-attacks, advanced tactics may evade detection. The proposed method provides a complementary, real-time detection layer, analyzing both physical and operational data to enhance system resilience and prevent misclassification. This innovative strategy comprises two distinct yet simultaneous approaches. The first approach involves extracting timing features (t_2 to t_5) from the data collected through online CB monitoring. These features are then positioned within a probability distribution curve to assess the health status of the CB. The second approach focuses on monitoring TKE, which is explicitly utilized to identify the cause of line outages and distinguish between faults and cyber-attacks. It is not employed to monitor the CB itself, which is managed through the time feature analysis.

The TKE within the power system is directly influenced by the difference in speed between the reference generator and the other generators. Usually, this speed difference is negligible during normal power system operation, making it almost negligible. However, due to the dynamic characteristics of renewable power systems, the TKE is not exactly zero. Consequently, in such scenarios, there will be slight fluctuations in the TKE. Therefore, the TKE will undergo slight variations. However, during faults and stressful situations in the power system, the synchronism between generators is disturbed at the moment the fault occurs, leading to an acceleration of the generators. Consequently, the TKE, which correlates directly with the square of the speed difference, undergoes a sudden change when a fault event occurs, following which it begins to decrease. If system stability is maintained, TKE remains at a minimum level; however, instability results in a subsequent increase. A sudden mutation in a short time means a significant increase in the time derivative $\left(\frac{d\text{TKE}}{dt}\right)$. The TKE behavior, as described, is being implemented for the first time as a criterion to identify faulty power systems, malfunctions in protection systems, and line outages, even in the absence of fault conditions. Following the investigation of fault existence, as previously discussed, this research concerns CB open without command failures. To achieve this, the timing features given in Table I are initially extracted through experimental tests on CBs. It is important to note that these timing attributes can be obtained from factory-provided data for recently installed circuit breakers. Moreover, in cases where there is a lack of adequate information, experimental tests can be employed. Subsequently, a probability distribution is constructed for each timing feature (t_2 to t_5). According to the probability distribution, the health condition can be assessed if the newly measured data falls within the healthy interval. In contrast, the alarm condition can be identified if it falls within the alarm interval. The alarm condition in time step t may result in failure in time step $t+1$. Therefore, alarm condition detection may help detect early failure. Fig. 5 shows the computational procedure of the proposed method.

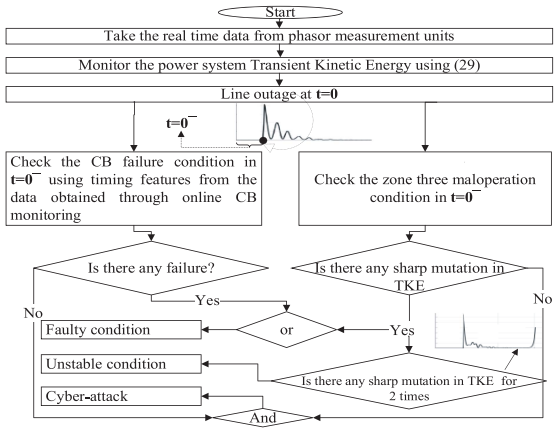

Fig. 5. Computational procedure of the proposed method.

IV. Practical Considerations

Practical implementation can be investigated by the following concerns.

1) Complexity in modeling for TKE calculation: The proposed method is model-free and does not necessitate intricate modeling for TKE calculation. Only real-time data from generation units is required to calculate the TKE using (29). It is worth mentioning that the proposed intricate two-axis model of SGs, combined with a static excitation system, was employed solely for accurately tracking the real-world system's behavior and providing more accurate simulation results.

2) Real-time data from generation units: In addressing concerns regarding the availability of necessary data for TKE monitoring, it's crucial to note that the existing SCADA monitoring system updates the event sequence every millisecond and acquires the necessary real-time data from PMUs. Consequently, the current SCADA systems effectively meet the conditions for real-time data requirements.
3) Availability of CB time features and real-time monitoring: These temporal attributes depend on the CB type and are either supplied by manufacturers or can be readily measured and documented before installation. Regarding real-time CB health condition monitoring, it is worth mentioning that industry leaders in this field are actively developing such features.
4) Applicability: The SCADA system is already equipped with numerous algorithms for analyzing system statuses based on the received information. Given the availability of relevant data within the SCADA system, our proposed methods can be integrated into existing infrastructure as a novel detection method.
5) Computational resource requirements and processing time estimates: The real-world implementation of the proposed method requires a standard SCADA workstation with an event-sequence update rate of 1 ms. For the processing time estimation, the rate of change of TKE is initially monitored. When it exceeds the maximum observed value under normal conditions, with an additional 10% margin for uncertainty, further monitoring is triggered. The processing time is then determined based on when the TKE surpasses the maximum value observed under normal conditions by an additional 10%, accounting for uncertainties.

The proposed method is designed to leverage current SCADA infrastructure, allowing seamless integration by utilizing real-time data from circuit breakers and generators without extensive modifications. It complements existing cybersecurity measures by providing an additional layer of detection for cyber-attacks, particularly targeting protection systems. By integrating with existing anomaly detection algorithms, the proposed approach enhances situational awareness and response times to potential threats. On the other hand, the model-free nature of our methodology ensures scalability and adaptability, making it compatible with various configurations.

V. Test Results and Discussion

To demonstrate the performance of the proposed method, a two-step process was followed. First, an experimental investigation was conducted to collect real-time data from a 170 kV circuit breaker, focusing on its health condition evaluation. Next, a modified renewable New England test system was simulated, incorporating the CB experimental data, to assess various fault scenarios and potential cyber-attacks. Finally, OPAL-RT HIL validation was performed to verify the Simulink simulation results.

A. Experimental Test Results

The experimental testbed for the 170kV circuit breaker is depicted in Fig. 6, revealing a comprehensive integration of sensors within both the control and operational components. These sensors are instrumental in facilitating online detection of the CB's health condition. Specifically, they monitor the CB coil trip current and contact travel curve during its open operation, offering invaluable data for early detection and prevention of failures. Fig. 7(a) showcases the experimental results of the coil current, while Fig. 7(b) illustrates the utilization of contact travel curves for detecting mechanical failures, particularly during open operation. Following each test iteration, timing features (t_2 to t_5) are extracted from the measured data. To ensure robustness and reliability, the experimental tests are repeated 100 times in this research. Based on the obtained results and the extracted features of each test, probability distribution curves for each feature are generated. These curves serve as crucial tools for further analysis and understanding of the CB's health condition.

Fig. 6. Testbed for the experimental CB health condition monitoring.

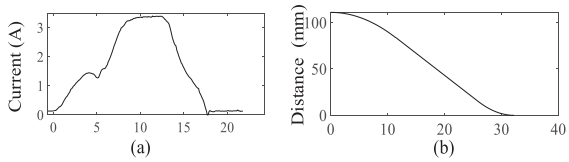

Fig. 7. Experimental result of CB. (a) Coil trip current. (b) Contact travel cure during CB open operation.

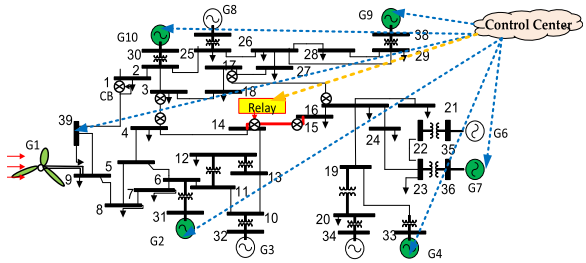

Fig. 8. Test system.

B. Numerical Simulation Results

A modified renewable 39-bus New England system, which includes data from [36], [41], as shown in Fig. 8, is used for this study. The DFIG parameters are provided in Table II. To synchronize with the time updates in SCADA, a sampling rate of 1ms was used for the variable computations in all the numerical simulations conducted within the MATLAB environment. In the test system, an aggregated model of a DFIG-based wind farm was additionally incorporated into Bus 9. The wind farm was conceptualized as a cohesive unit, akin to a single machine, due to the integration of multiple wind turbines. The fundamental operational aspects of the power system incorporating wind

TABLE II
DFIG PARAMETERS USED IN THE STUDY

Parm	Values [pu]	Parm	Values	Parm	Values
L_m	4	H_t	4 [s]	H_g	$0.1 \times H_t$ [s]
L_{ss}	$1.01 \times L_m$	K	0.3[pu/el.rad]	$P_{tw,rated}$	5 [MW]
L_{rr}	$1.005 \times L_{ss}$	C	0.01[pu/el.rad]	R	40.05 [m]
r_s	0.005	β	0	ρ	1.225 [kg/m^3]
r_r	$1.1 \times r_s$	V_m	15 [m/s]	N	222

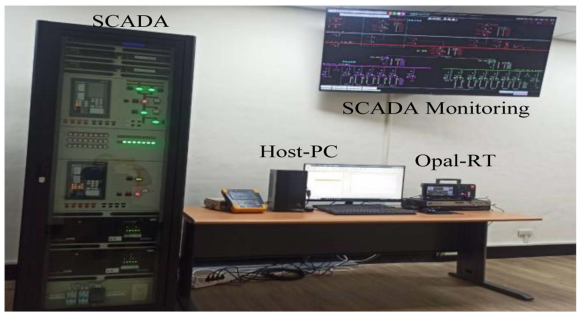

Fig. 9. Hardware-in-the-loop testbed.

power have been taken into account. Time-domain simulation is conducted using a simultaneous implicit approach in accordance with power system modeling for the calculation of the accurate trajectory of the generator angle, which is used for TKE monitoring. In steady-state operating conditions, the system dynamics were simulated to have a time response of 10 s before the fault manifests itself.

Experimental and simulation studies have been carried out in four different scenarios to evaluate the validity of the proposed method. In Scenario 1, the effect of stable and unstable faults on TKE variation has been studied. Scenario 2 focuses on identifying false trips, stable and unstable power swing conditions, and overloading. An unplanned false line trip due to malicious cyber-attacks has been studied in Scenario 3. Scenario 4 investigates two-line outage events, where the first line outage is due to the cyber-attack, while the second line outage is due to faults. In all scenarios, the three-phase short circuit fault is used to simulate renewable power system faults. Although there is no difference between the types of faults from a TKE perspective, each fault increases TKE. The Opal-RT was employed as a hardware-in-the-loop system to validate the results. The hardware-in-the-loop testbed is illustrated in Fig. 9.

In Scenario 1, it is assumed that a fault occurs between buses 14 and 15, and it is fixed by cutting the line. The T-D simulation is carried out in this manner, and the curves of the rotor angle, active power of the SGs, and TKE are shown in Figs. 10 and 11. According to the T-D simulation results in Figs. 10 and 11, the system is stable when the fault clearing time is set to 0.198 s and unstable at 0.199 s. As a result, the critical clearing time is 0.198–0.199 s. From Fig. 10(c) and Fig. 11(c), the TKE variation during system faults can be observed. The TKE also has negligible variations during normal conditions because the renewable smart power system is dynamic. It can be seen that, at the moment of the fault, the TKE increases sharply. This indicates that a sudden mutation occurs in the TKE time derivative ($\frac{d\text{TKE}}{dt}$) at this time. Referring to Fig. 11(c), it becomes evident that the TKE has undergone two distinct mutations. The first mutation corresponds to the fault occurrence, while the second mutation is attributed to system instability. It can be observed that the rate

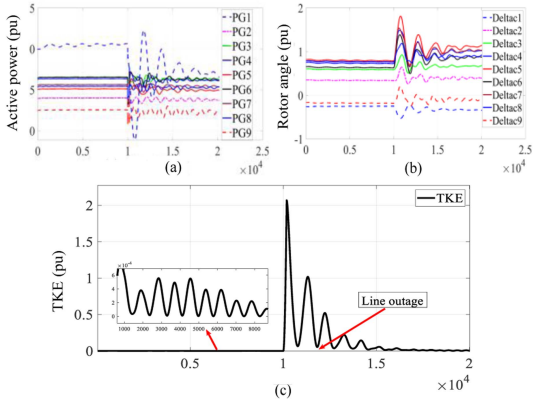

Fig. 10. Power system stable condition. (a) Active power. (b) Rotor angle (c) TKE.

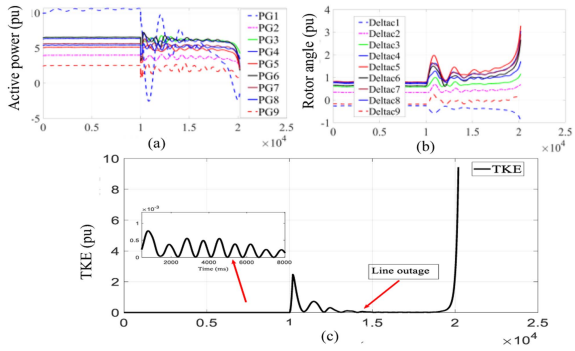

Fig. 11. Power system unstable condition. (a) Active power. (b) Rotor angle. (c) Transient kinetic energy.

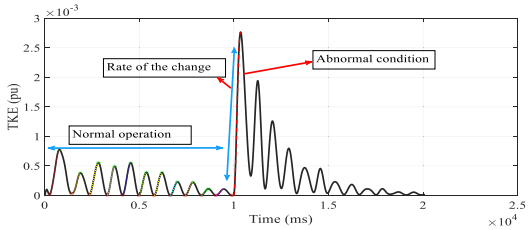

Fig. 12. TKE for statistical analysis.

of change of mutation ($\frac{d\text{TKE}}{dt}$) is comparatively lower during the second mutation.

To evaluate the dynamics of TKE within the power system, a statistical analysis was undertaken. This analysis investigated the behavior of TKE under both normal and abnormal conditions. For each scenario, the minimum and maximum TKE values were identified, and these points were connected with a line, as illustrated in Fig. 12.

Following this graphical representation, the rate of change and the discrepancy between the TKE values as well as statistical values such as mean, standard deviation, and confidence interval of 95% are computed and presented in Table III. Statistical comparison of TKE behavior under normal and abnormal conditions in a power system, as provided in Table III, clearly shows distinct differences. The confidence interval analysis reveals that the lowest rate of change in TKE under abnormal conditions, within the 95% confidence interval, is more than eight times greater than the highest rate of change within the 95%

TABLE III
FEATURES FOR TKE

NORMAL CONDITION					
Rate of change for each swing			Differences (Max_{value}-Min_{value}) in TKE for each swing × $1e^{-3}$		
0.0017	0.000745	0.000894	0.7599	0.3464	0.5405
0.0012	0.0012	0.000972	0.4835	0.5412	0.3868
0.000927	0.000596	0.000541	0.3847	0.2284	0.2207
0.000291	0.000259		0.1092	0.1075	
Mean= 8.48× $1e^{-4}$			Mean= 0.374 × $1e^{-3}$		
Standard deviation= 4.27× $1e^{-4}$			Standard deviation= 0.201× $1e^{-3}$		
95% Confidence interval					
Rate of change for each swing			(0.5906 to 1.1346)× $1e^{-3}$		
Differences in TKE			(0.2386 to 0.5085)× $1e^{-3}$		
ABNORMAL CONDITION					
Rate of change=0.0093			Difference in TKE= 2.8×$1e^{-3}$		
95% Confidence interval from different Scenarios					
Rate of change for each swing			(8.884 to 9.92)× $1e^{-3}$		
Differences in TKE			(2.65 to 2.87)× $1e^{-3}$		

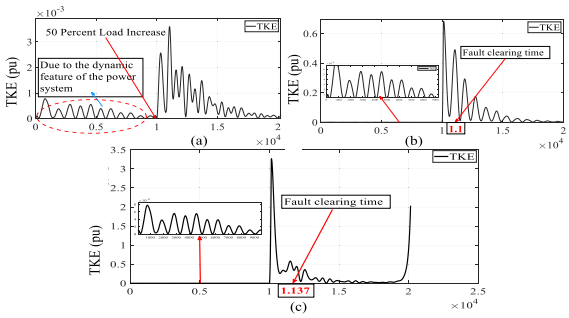

Fig. 13. Transient kinetic energy variation. (a) Overloading. (b) Stable power swing. (c) Unstable power swing.

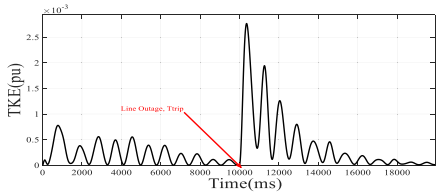

Fig. 14. TKE monitoring in Scenario 3.

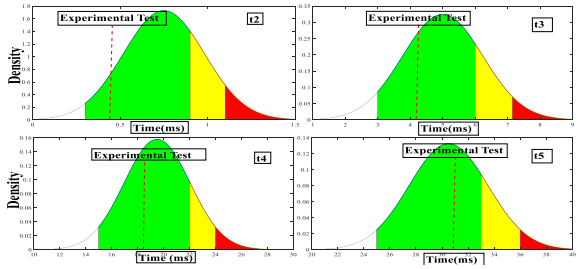

Fig. 15. Experimental test results for CB failure monitoring in Scenario 3.

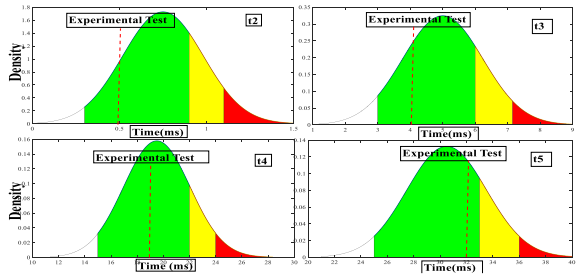

Fig. 16. Experimental test results for CB failure monitoring in Scenario 4.

confidence interval for normal conditions, indicating substantial variations in $\frac{d\text{TKE}}{dt}$. Furthermore, the 95% confidence interval for the difference between the maximum and minimum TKE values indicates that the smallest difference under abnormal conditions is more than five times larger than the largest difference observed under normal conditions. Considering the method conditions for computational resource requirements and processing time estimates, the processing time in this case study is conservatively estimated at 100 ms.

The effectiveness of the proposed TKE strategy in detecting zone three maloperations has been provided in Scenario 2. To achieve this objective, a study was conducted to analyze the impact of stable and unstable power swing conditions, as well as overloading scenarios, which have been identified as potential causes of malfunctions in distance relays' zone three operations. As discussed, these conditions happen when the system is under stress following a fault. Considering a symmetrical fault on a transmission line between buses 14 and 15, a stable power swing condition was established. The issue was initiated at 10 s and resolved at 10.1 s. For unstable power swing conditions, the fault was cleared 1.137 s later (at 11.137 s). For load encroachment conditions, the load at bus 12 was increased by 50% at 10 s. Fig. 13 shows the TKE variation under these conditions. It can be seen from Fig. 13 that how TKE monitoring can detect any of the above stress factors that can cause a line outage. From Scenarios 1 and 2, it is concluded that in faulty and stressful conditions, the TKE experiences a sharp mutation at first; then, the line outage happens. Consequently, a delay exists between the sharp TKE mutation and the onset of the line outage. In Scenario 3, an attacker with remote access is responsible for triggering an unplanned outage on the line between buses 14 and 15.

The line outage moment is called T_{trip}. The proposed algorithm uses TKE and online CB monitoring for anomaly detection, as shown in Figs. 14 and 15. It can be seen from Fig. 14 that at T_{trip}, the TKE has significantly increased. It means that there is no delay between the sharp TKE mutation and the onset of the line outage. Therefore, it can be concluded power system faults and stresses are not the reason for the line outage. As a result, it may be related to CB failure. The experimental findings depicted in Fig. 15 reveal that the CB is operating under normal and healthy conditions.

In Scenario 4, a hypothetical situation is presented where a cyber assailant with remote access intentionally triggers an unplanned line trip on the interconnecting line between buses 14 and 15. Subsequently, another line experiences an interruption shortly afterward due to a fault. The test results shown in Figs. 16 and 17 depict the experimental CB online monitoring and TKE variations. For the analysis of the first line outage, it is evident from Fig. 17 that there is a substantial increase in kinetic energy at T_{trip}. This suggests that there is no temporal gap between the occurrence of the abrupt TKE mutation and the initiation of the line outage. Therefore, it can be inferred that power system failures and stress conditions do not serve as the underlying cause of the line outage. In the case of the second line outage,

TABLE IV
FEATURE COMPARISONS

Aspects	Proposed Method	Observer-Based Method [8, 36]	Neural Network Approach [17]	Signature-Based Approach [14]	Anomaly-Based Approach [18]
Approach	Monitors and analyzes waveform	Monitors and analyzes system behavior	Uses neural networks for pattern recognition and learning to classify event	Matches known attack signatures to identify threats	Identifies deviations from established baselines
Detection Mechanism	Employs the TKE technique and real-time monitoring of CBs	Sliding mode control observer.	Employs artificial neural networks for complex pattern recognition	Recognizes predefined patterns associated with known threats	Detects anomalies by unknown input observer
Real-time Processing	Real-time	Real-time	Real-time detection, but not for new case studies.	Real-time	Real-time.
Adaptability	Generally, adapts	Regular updates required for rule adaptation	Adapts through training on new data suitable for evolving threats.	Requires constant updates for new attack signatures.	Adapts.
False Positive Rates	low false positives	Prone to false positives, especially with rule sensitivity	Can be sensitive to the quality and quantity of training data	Generally low false positives	if normal behavior patterns change
Ease of Integration	Relatively easy to integrate into existing SCADA systems	Easier to integrate into existing security infrastructures	Integration may require specialized knowledge but can be incorporated into existing systems	Relatively easy to integrate into existing systems with signature databases	Integration may require adapting to changing network patterns.
Robustness Against Stealthy Attacks	Robust	Vulnerable	Vulnerabilities to new adversarial attacks	Effective against known threats, vulnerable to zero-day attacks	May struggle with new, sophisticated attacks
Dependency on System Model	No	Yes	No	No	Yes
Computational Cost	Low	Moderate to High	High	Low to Moderate	Moderate to High
Potential Limitations	Sensitivity to system dynamics and integration with current grid infrastructures	Struggles with rapid system changes and evolving attacks	Requires substantial training data and is computationally expensive for real-time adaptation	Ineffective against unknown or zero-day attacks without new signatures	May fail to detect stealthy attacks due to dependency on predefined patterns

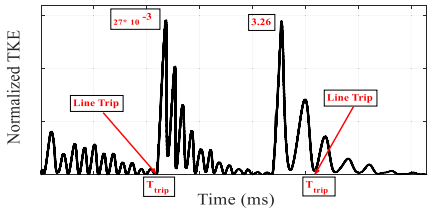

Fig. 17. TKE monitoring in Scenario 4.

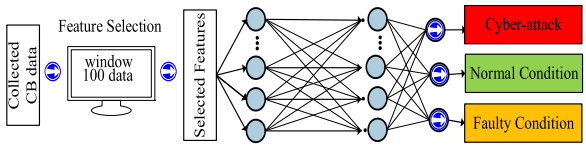

Fig. 18. Trained RBFN.

it is apparent that prior to the event, there was a significant rise in kinetic energy. This implies the existence of a temporal gap between the occurrence of the abrupt TKE mutation and the initiation of the line outage. Consequently, it can be inferred that power system problems are the underlying cause of the line outage. In both instances, the experimental test findings depicted in Fig. 16 demonstrate a state of good health.

In comparison with some well-known detection methods, the proposed method utilizes a direct waveform analysis, however, neural network methods learn patterns from data to classify events, observer detection methods monitor system variables and identify anomalies to detect cyber-attacks or faults, signature-based approaches identify known patterns or signatures of cyber-attacks within the system, and anomaly-based approaches detect abnormalities by identifying deviations from expected patterns. Therefore, the response time in neural network methods depends on the complexity of the network and the computational resources available. In observer detection methods, the response time relies on the complexity of the observer algorithm and the speed of data processing; the signature-based approaches may offer real-time capabilities depending on the efficiency of signature matching algorithms; in anomaly-based approaches, the response time depends on the complexity of anomaly detection algorithms and the speed of data processing. Regarding adaptability, the proposed method is adaptable to different power system configurations and operational conditions. Although the other methods may require adjustments or fine-tuning based on specific system configurations or changes in operating conditions. Unlike the mentioned methods that may require updates to address new cyber-attack patterns, the proposed method uses direct TKE analysis, which is driven by actual system faults and generator speeds, eliminating the need for updates. Additionally, the proposed method does not depend on historical data for training, leading to reduced computational time and costs. Table IV compares the proposed method with other well-known methods

To assess the effectiveness of the proposed method, a RBFN is utilized for comparison. This network is popular due to its faster process, reduced overfitting with ability to handle large and complex datasets [42]. The RBFN has been designed to differentiate between normal, faulty, and cyber-attack cases. Fig. 18 illustrates the structure of the designed RBFN. In the data collection process for each scenario (normal, faulty, and under cyber-attack), the TKE variation, as well as timing features of CB (t1 to t5), are collected from 1000 time runs with a resolution of one millisecond. After that, in a window of 100 samples, the features are extracted. The features are mean, mode, median,

standard deviation, skewness, variance, summation, quantiles (25th and 75th), kurtosis, maximum, minimum, as well as the rate of the change to track the $\frac{d\text{TKE}}{dt}$. The RBFN structure was employed and consisted of three layers, including input, hidden, and output. The input layer receives data collected from various scenarios, with each node representing a single feature and accepting its corresponding input value, resulting in a total of 14. The hidden layer contains a set of radial basis functions that are used to map the input data into a higher dimensional feature space, a total of 8 neurons. Each node in this layer applies a radial basis function to the input data, producing a scalar output, and utilizes the Gaussian function as the activation function. In the output layer, the final network output classifies input data as normal or anomalous, with one node representing normal data and the other anomalous. In this article, SoftMax is utilized as the activation function, and backpropagation supervised learning techniques enable training. The network is trained by using a set of labeled data to adjust the weights, minimizing classification errors. In the dynamic renewable power system, the TKE undergoes continuous fluctuations, as illustrated in Fig. 13(a). These variations pose challenges for RBFN detections, introducing errors. To enhance accuracy, the window size was reduced, focusing on improved feature selection, particularly emphasizing the rate of change of TKE and its maximum values within each window. These adjustments have indeed improved the detection capabilities while increasing the computational costs. Consequently, the computational time, cost, and complexity associated with the RBFN are significantly greater than those of the proposed methodology based on waveform analysis. This disparity necessitates a high-processing hardware infrastructure and substantial resources to manage the processing requirements effectively. This limitation raises concerns regarding its effectiveness in real-time and critical applications, where rapid response to cybersecurity threats is essential for maintaining the integrity and reliability of intelligent power systems. In contrast, the proposed method not only streamlines computational efficiency but also enhances the real-time identification of the root causes of line outages, thereby significantly improving the overall cybersecurity posture of power systems.

VI. Conclusion

A unique methodology has been suggested to detect stealthy cyber-attacks, focusing on the examination of transient kinetic energy waveforms and the implementation of real-time monitoring of circuit breakers. This novel approach can be seamlessly integrated into SCADA systems to enable timely detection of the underlying causes of line outages. The efficacy of this approach has been verified and showcased through extensive time-domain simulations conducted on the modified New England 39-bus system, which integrates wind farm data and experimental tests. The testing results and comparison with RBFN confirm the robustness of this approach against surreptitious cyber-attacks targeting protection systems. The examination of waveforms representing TKE reveals a noteworthy observation that during abnormal conditions, the rate of change in TKE is more than several times faster than under normal conditions. Furthermore, in the presence of faults, there is an observable time delay between the occurrence of a sudden change in TKE and the onset of a line outage. Nevertheless, the absence of this delay is observed in stealthy cyber-attacks and circuit breaker failures. These key observations indicate that the behavior of the system remains unaffected by the specific nature of the cyber-attack. Therefore, the proposed method can detect all types of cyber-attacks that cause false trips. The compression with RBFN validates the performance of the proposed method**.** Considering the increasing penetration of converter-based renewable energy sources integrated with virtual inertia strategies, improving the proposed method for such power systems is suggested for future studies.

References

[1] A. M. Abdullah and K. Butler-Purry, "Distance protection zone 3 misoperation during system wide cascading events: The problem and a survey of solutions," *Elect. Power Syst. Res.*, vol. 154, pp. 151–159, 2018.

[2] P. Dehghanian, Y. Guan, and M. Kezunovic, "Real-time life-cycle assessment of high-voltage circuit breakers for maintenance using online condition monitoring data," *IEEE Trans. Ind. Appl.*, vol. 55, no. 2, pp. 1135–1146, Mar./Apr. 2019.

[3] M. Kezunovic et al., "Automated monitoring and analysis of circuit breaker operation," *IEEE Trans. Power Del.*, vol. 20, no. 3, pp. 1910–1918, Jul. 2005.

[4] Y. Lu and Y. Li, "A novel fault diagnosis method for circuit breakers based on optimized affinity propagation clustering," *Int. J. Elect. Power Energy Syst.*, vol. 118, 2020, Art. no. 105651.

[5] H. K. Hoidalen and M. Runde, "Continuous monitoring of circuit breakers using vibration analysis," *IEEE Trans. Power Del.*, vol. 20, no. 4, pp. 2458–2465, Oct. 2005.

[6] S. H. Rouhani, E. Abbaszadeh, M. A. Sepestanaki, S. Mobayen, C. L. Su, and A. Nemati, "Adaptive Finite-time tracking control of fractional microgrids against time-delay attacks," *IEEE Trans. Ind. Appl.*, vol. 60, no. 2, pp. 2153–2164, Mar./Apr. 2024.

[7] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4332–4341, Jul. 2019.

[8] S. H. Rouhani, H. Mojallali, and A. Baghramian, "Load frequency control in the presence of simultaneous cyber-attack and participation of demand response program," *Trans. Inst. Meas. Control*, vol. 44, no. 10, pp. 1993–2011, 2022.

[9] A. A. Jahromi, A. Kemmeugne, D. Kundur, and A. Haddadi, "Cyber-physical attacks targeting communication-assisted protection schemes," *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 440–450, Jan. 2020.

[10] M. Rajaee and K. Mazlumi, "Multi-agent distributed deep learning algorithm to detect cyber-attacks in distance relays," *IEEE Access*, vol. 11, pp. 10842–10849, 2023.

[11] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3104–3113, Nov. 2015.

[12] S. H. Rouhani, H. Mojallali, and A. Baghramian, "An optimized fuzzy sliding based active disturbance rejection control for simultaneous cyber-attack tolerant and demand response participation program," *Int. Trans. Elect. Energy Syst.*, vol. 31, no. 12, 2021, Art. no. e13206.

[13] J. Hong, R. Karnati, C. W. Ten, S. Lee, and S. Choi, "Implementation of secure sampled value (SeSV) messages in substation automation system," *IEEE Trans. Power Del.*, vol. 37, no. 1, pp. 405–414, Feb. 2022.

[14] M. Yousefi kia, M. Saniei, and S. G. Seifossadat, "A novel cyber-attack modelling and detection in overcurrent protection relays based on wavelet signature analysis," *IET Gener., Transmiss. Distrib.*, vol. 17, no. 7, pp. 1585–1600, 2023.

[15] R. Li, Z. Wang, L. Fang, C. Peng, W. Wang, and H. Xiong, "Efficient blockchain-assisted distributed identity-based signature scheme for integrating consumer electronics in metaverse," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 3770–3780, Feb. 2024.

[16] Q. Xie et al., "LiteCrypt: Enhancing IoMT security with optimized HE and lightweight dual-authorization," in *Proc. IEEE 30th Int. Conf. Parallel Distrib. Syst.*, 2024, pp. 166–175.

[17] S. Pola, M. Jovanovic, M. Azzouz, and M. Mirhassani, "Cyber resiliency enhancement of overcurrent relays in distribution systems," *IEEE Trans. Smart Grid*, vol. 15, no. 4, pp. 4063–4076, Jul. 2024.

[18] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1636–1646, May 2018.
[19] M. Pasetti et al., "Artificial neural network-based stealth attack on battery energy storage systems," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5310–5321, Nov. 2021.
[20] A. Ameli, A. Hooshyar, E. F. El-Saadany, and A. M. Youssef, "Attack detection and identification for automatic generation control systems," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4760–4774, Sep. 2018.
[21] M. N. Kurt, Y. Yılmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 2, pp. 498–513, 2019.
[22] A. Takiddin, S. Rath, M. Ismail, and S. Sahoo, "Data-driven detection of stealth Cyber-attacks in DC microgrids," *IEEE Syst. J.*, vol. 16, no. 4, pp. 6097–6106, Dec. 2022.
[23] R. M. G. Ferrari and A. M. H. Teixeira, "A switching multiplicative watermarking scheme for detection of stealthy cyber-attacks," *IEEE Trans. Autom. Control*, vol. 66, no. 6, pp. 2558–2573, Jun. 2021.
[24] P. C. Magnusson, "The transient-energy method of calculating stability," *Trans. Amer. Inst. Elect. Engineers*, vol. 66, no. 1, pp. 747–755, 1947.
[25] M. R. Barzegar-Bafrooei and A. A. Foroud, "Investigation of the performance of distance relay in the presence of saturated iron core SFCL and diode bridge type SFCL," *Int. Trans. Elect. Energy Syst.*, vol. 29, no. 2, 2019, Art. no. e2736.
[26] S. R. Mohanty, V. R. Pandi, B. K. Panigrahi, N. Kishor, and P. K. Ray, "Performance evaluation of distance relay with CT saturation," *Appl. Soft Comput.*, vol. 11, no. 8, pp. 4789–4797, 2011.
[27] A. H. Abu Bakar, S. A. Khan, T. C. Kwang, and N. A. Rahim, "A review of ferroresonance in capacitive voltage transformer," *IEEJ Trans. Elect. Electron. Eng.*, vol. 10, no. 1, pp. 28–35, 2015.
[28] S. Rezaei, "Behavior of protective relays during subsynchronous resonance in transmission line and adaptation of generator out-of-step protection," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 5687–5698, Nov./Dec. 2019.
[29] A. Heidary, K. Rouzbehi, H. Radmanesh, and J. Pou, "Voltage transformer ferroresonance: An inhibitor device," *IEEE Trans. Power Del.*, vol. 35, no. 6, pp. 2731–2733, Dec. 2020.
[30] K.-H. Tseng and P.-Y. Cheng, "Mitigating 161kV electromagnetic potential transformers' ferroresonance with damping reactors in a gas-insulated switchgear," *IET Gener., Transmiss. Distrib.*, vol. 5, no. 4, pp. 479–488, 2011.
[31] S. Rezaei, "An adaptive bidirectional protective relay algorithm for ferroresonance in renewable energy networks," *Elect. Power Syst. Res.*., vol. 212, 2022, Art. no. 108625.
[32] A. A. Fouad and V. Vittal, "The transient energy function method," *Int. J. Elect. Power Energy Syst.*, vol. 10, no. 4, pp. 233–246, 1988.
[33] H. R. Shabani, M. Kalantar, and A. Hajizadeh, "Real-time transient instability detection in the power system with high dfig-wind turbine penetration via transient energy," *IEEE Syst. J.*, vol. 16, no. 2, pp. 3013–3024, Jun. 2022.
[34] P. Ledesma and J. Usaola, "Doubly fed induction generator model for transient stability analysis," *IEEE Trans. Energy Convers.*, vol. 20, no. 2, pp. 388–397, Jun. 2005.
[35] A. Mitra and D. Chatterjee, "A sensitivity based approach to assess the impacts of integration of variable speed wind farms on the transient stability of power systems," *Renewable Energy*, vol. 60, pp. 662–671, 2013.
[36] H. R. Shabani and M. Kalantar, "Real-time transient stability detection in the power system with high penetration of DFIG-based wind farms using transient energy function," *Int. J. Elect. Power Energy Syst.*, vol. 133, 2021, Art. no. 107319.
[37] F. Mei and B. Pal, "Modal analysis of grid-connected doubly fed induction generators," *IEEE Trans. Energy Convers.*, vol. 22, no. 3, pp. 728–736, Sep. 2007.
[38] A. Mitra and D. Chatterjee, "Active power control of dfig-based wind farm for improvement of transient stability of power systems," *IEEE Trans. Power Syst.*, vol. 31, no. 1, pp. 82–93, Jan. 2016.
[39] J. Zhong, W. Li, R. Billinton, and J. Yu, "Incorporating a condition monitoring based aging failure model of a circuit breaker in substation reliability assessment," *IEEE Trans. Power Syst.*, vol. 30, no. 6, pp. 3407–3415, Nov. 2015.
[40] A. P. Purnomoadi, A. R. Mor, and J. J. Smit, "Spacer flashover in gas insulated switchgear (GIS) with humid SF6 under different electrical stresses," *Int. J. Elect. Power Energy Syst.*, vol. 116, 2020, Art. no. 105559.
[41] M. A. Chowdhury, W. Shen, N. Hosseinzadeh, and H. R. Pota, "Transient stability of power system integrated with doubly fed induction generator wind farms," *IET Renewable Power Gener.*, vol. 9, no. 2, pp. 184–194, 2015.
[42] Y. Sun, J. Xu, G. Lin, W. Ji, and L. Wang, "RBF neural network-based supervisor control for maglev vehicles on an elastic track with network time delay," *IEEE Trans. Ind. Inform.*, vol. 18, no. 1, pp. 509–519, Jan. 2022.

Seyed Hossein Rouhani (Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Guilan, Rasht, Iran, in February 2022.

He subsequently worked as a Postdoctoral Researcher with the Department of Electrical Engineering, National Kaohsiung University of Science and Technology, Kaohsiung, Taiwan, where he is currently serving as an Assistant Professor. His research interests include renewable energy systems, smart power system analysis, cybersecurity, control, and system stability. He is particularly focused on enhancing the cybersecurity of power systems by integrating the dynamic characteristics of power system operations into detection and mitigation frameworks. He is actively exploring novel methodologies to address cybersecurity challenges by leveraging the dynamic behavior of power systems as a new perspective for identifying and counteracting cyber threats.

Dr. Rouhani contributes to the academic community as an Associate and Guest Editor for several specialized scientific journals and has authored numerous peer-reviewed publications.

Chun-Lien Su (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from National Sun Yat-Sen University, Kaohsiung, Taiwan, in 2001.

He has been with the National Kaohsiung Marine University, Kaohsiung, as a Full Professor since 2012. He was a Visiting Professor with Aalborg University, Denmark, in 2017, and later served as the Director of the Maritime Training Center, National Kaohsiung University of Science and Technology (NKUST), Kaohsiung, Taiwan. Since 2021, he has been a Distinguished Professor with the Department of Electrical Engineering, NKUST and the Director of the Center for Electrical Power and Energy. His research interests include renewable power system, power quality, microgrids, and offshore energy systems, especially electrical infrastructure for offshore wind farms and maritime applications.

Dr. Su served as the Guest Editor and Associate Editor for prestigious IEEE and IET journals.

Hamid Reza Shabani received the Ph.D. degree in power electrical engineering from the Iran University of Science and Technology, Tehran, Iran, in 2021.

He has also worked as a Postdoctoral Researcher with Aalborg University (AAU Energy) for about one year. His research interests include power system stability, power system dynamic and control, and renewable energies.

Mostafa Esmaeili Shayan received the M.Sc. (Hons.) and Ph.D. degrees in renewable energy engineering from Tarbiat Modares University, Tehran, Iran, in 2017 and 2022, respectively.

Following his studies, he was appointed the Director of the Engineering Division at Saba Power and Energy Group, the largest private electric power company in Iran, where he served for two years. Since early 2024, he has been serving as a Postdoctoral Researcher with the Department of Mechanical, Chemical, and Materials Engineering, Università degli Studi di Cagliari, Cagliari, Italy. His current research focuses on optimizing integrated energy systems for the supply of electricity, heating, and cooling in both European and African contexts. He actively contributes to the academic community as an editor for several specialized scientific journals and has authored numerous impactful publications. His research interests include energy conversion, system optimization, solar and wind energy, advanced energy storage technologies, and electric vehicles.

Saleh Mobayen (Senior Member, IEEE) received the Ph.D. degree in control engineering from Tarbiat Modares University, Tehran, Iran, in 2013.

He was with the University of Zanjan, Zanjan, Iran. He is an Associate Professor with the Graduate School of Intelligent Data Science, National Yunlin University of Science and Technology (YunTech), Douliou, Taiwan. His research interests include artificial intelligence, control theory, nonlinear and robust systems, sliding mode and finite-time control, with applications in robotics, UAVs, communication, and cyber-physical systems. He has published more than 300 papers in top-tier journals, including 15+ in *IEEE Transactions*, and supervised more than 60 graduate students. He serves as editorial and reviewer roles across 40+ high-impact journals.

Dr. Mobayen is a frequent keynote and invited speaker, and the founder of ACSLab at both ZNU and YunTech, promoting international collaboration and applied control research. As ESI/ISI highly-cited researcher, he has ranked among the world's top 1% researchers (2020–2024) and was awarded Taiwan's Research Excellence Award in 2023.

Navid Razmjooy (Senior Member, IEEE) received the Ph.D. degree in electrical engineering (control and automation) from Tafresh University, Tafresh, Iran, in 2018.

He also completed a research fellowship at the Amirkabir University of Technology from 2017 to 2018. He currently serves as an Adjunct Professor with the Saveetha School of Engineering, SIMATS, India. He is known for developing the FIFA World Cup Optimization Algorithm and applying it in areas such as medical diagnostics, smart energy systems, and industrial automation. Recognized among the world's top 2% of scientists by Stanford University and Scopus, he integrates artificial intelligence and optimization techniques to enhance the performance and reliability of energy systems, medical imaging, and control applications. His impactful contributions bridge academic research and practical technological solutions across multiple fields. His research interests include renewable energy systems, metaheuristic optimization, soft computing, image processing, machine vision, and interval analysis.

Jin-Ting Yu (Student Member, IEEE) received the bachelor's and master's degrees in marine engineering from National Kaohsiung Marine University, Kaohsiung, Taiwan, in 2012 and 2015, respectively. He is currently working toward the Ph.D. degree in the electrical engineering Department, National Kaohsiung University of Science and Technology, Kaohsiung in 2020. He is now a student chair at the IEEE NKUST Student Branch

His research interests include power system quality, renewable energy, and ship microgrids.

Chih-Yuan Chiang received the M.S. degree in electrical engineering from the National Cheng Kung University, Tainan, Taiwan, in 2015. He is currently working toward the Ph.D. degree in electrical engineering from the National Kaohsiung University of Science and Technology, Kaohsiung, Taiwan.

He worked for Taiwan Semiconductor Manufacture Company, Tainan, from May 2000 to May 2005 for extra-voltage, high voltage, low voltage inspection and maintenance, and SCADA integration. His research interests include real-time life-cycle assessment of high-voltage circuit breakers.