Model-Based Detection Scheme for Spoofed Sensor Data in Grid-Connected Inverters

Jinan Zhang, *Graduate Student Member, IEEE*, Mateo D. Roig Greidanus, *Graduate Student Member, IEEE*, Sudip K. Mazumder, *Fellow, IEEE*, Jin Ye, *Senior Member, IEEE*, Wenzhan Song, *Senior Member, IEEE*, and Homer Alan Mantooth, *Fellow, IEEE*

***Abstract*—In this article, a novel method to detect spoofed sensor data (SSD) for grid-connected inverters is proposed. First, a Kalman filter is used to estimate the inverter status in the proposed method. Then, the impact of SSD on the residual between estimation and control reference is analyzed. By leveraging the standard error of residual, an adaptive cumulative sum (CUSUM) chart is developed to achieve fast SSD detection and improve robustness. In addition, the proposed SSD detection method is verified by the hardware experiment. A comparative experiment with a conventional method also demonstrates the rapidity and robustness of the proposed method. Finally, the performance of the proposed method under different noise covariance matrices is analyzed. Comprehensive analysis shows that the proposed method meets the detection requirement in IEEE 1547 Standard.**

***Index Terms*—Adaptive cumulative sum chart (CUSUM), detection, grid-connected inverter, Kalman filter, spoofed sensor data (SSD).**

I. Introduction

THE cyber-physical security of modern renewable energy conversion systems has been one of the challenges in smart grid [1]. As they integrate data sensing, processing, and control, power electronic inverters are vulnerable to attackers with technical knowledge. For instance, noninvasive sensor spoofing attacks are used in [2] to compromise the performance of an inverter. With antennas and amplifiers, the spoofed sensor data (SSD) can be injected to destabilize the control system with devastating physical effects [3]. In [4], the impact of high-frequency noise injection due to aliasing on the detrimental performance of a grid-forming inverter is demonstrated.

Many intrusion detection methods have recently been developed to detect false data or SSD. Data-driven strategies show promise in anomaly detection without using any physical model information; however, they require a large amount of training data that is usually unavailable in real-world applications. Unlike data-driven methods, model-based detection methods employ the residual between measurement and estimation using physical model information to detect anomalies. For instance, the invariants are extracted from the model of both the physical system and controller to detect false data in the dc microgrid [5]. Our previous work [4] presented a detection and mitigation technique using a Kalman filter. The method was designed to deal with high-frequency SSD with subharmonic effects in the inverter. To cope with potential low-frequency SSD, a model-based detection method is developed in this letter. The main contributions are summarized as follows.

1) A novel fast, robust SSD detection method using a Kalman filter and adaptive cumulative sum (CUSUM) chart is proposed for the grid-connected inverter.
2) The proposed detection method is validated by a hardware experiment. The superior performance of the proposed method in terms of response time and robustness is also verified by comparative experiments with a conventional method.
3) A comprehensive analysis demonstrates the effectiveness of the proposed method in low-frequency SSD detection. The detection time also meets the requirements in IEEE 1547 Standard [6].

II. SSD Detection in Grid-Connected Inverter

A. SSD Representation

SSD is depicted as an additive signal to the measured data, which is given by $y_f = y_o + \beta$, where y_f is the compromised sensor data, which is the final input of the controller, y_o is the original measured data, β represents the spoofed sensor data. In this manuscript, three assumptions are made regarding the

Manuscript received 6 November 2022; revised 23 February 2023; accepted 28 March 2023. Date of publication 11 April 2023; date of current version 14 September 2023. This work was supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technologies Office under Award DE-EE0009026. The work of UIC's was supported by the U.S. Department of Energy's under Awards DE-EE0009026 and DE-CR0000019. *(Corresponding author: Jin Ye.)*

Jinan Zhang, Jin Ye, and Wenzhan Song are with the Center for Cyber-Physical Systems, University of Georgia, Athens, GA 30602 USA (e-mail: jinan.zhang@uga.edu; jin.ye@uga.edu; wsong@uga.edu).

Mateo D. Roig Greidanus and Sudip K. Mazumder are with the Electrical and Computer Engineering Department, University of Illinois Chicago, Chicago, IL 60607 USA (e-mail: mgreid2@uic.edu; mazumder@uic.edu).

Homer Alan Mantooth is with the Department of Electrical Engineering, University of Arkansas, Fayetteville, AR 72701 USA (e-mail: mantooth@uark.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIE.2023.3265059.

Digital Object Identifier 10.1109/TIE.2023.3265059

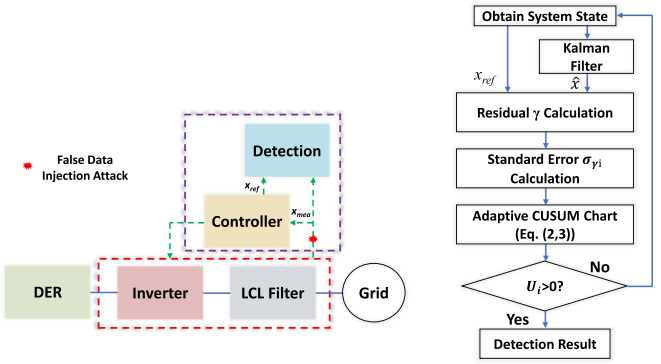

Fig. 1. (a) Diagram of the inverter with SSD detection. (b) Flowchart of SSD detection.

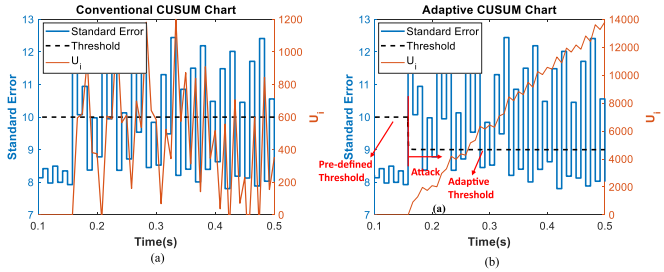

Fig. 2. (a) CUSUM chart. (b) Adaptive CUSUM chart.

cybersecurity of the grid-connected inverter. First, it is assumed that the cyber-network security is assured, making it difficult for attackers to corrupt the firmware and change the detection threshold in the microcontroller. Second, it is assumed that SSD injection cannot corrupt the firmware and only changes the inverter state by compromising the sensor measurement. Third, the proposed detection algorithm is considered to be trustworthy, which only uses local measurements to detect SSD.

B. Model-Based SSD Detection

The novel intrusion detection scheme proposed in this work is illustrated in Fig. 1(a). Fig. 1(b) introduces the Kalman filter role for the inverter state estimation. The estimator modeling has been developed in our previous work [4]. Although the high-frequency SSD has been addressed in that work, the potential low-frequency SSD effects are still a threat open to discussion for the grid-connected inverter, which is investigated in this manuscript.

To estimate the impact of low-frequency SSD, the residual is analyzed between the estimation and the reference controller, which is expressed as $\gamma = \frac{x_{ref}-\hat{x}}{x_{ref}}(\%)$, where $\hat{x}$ is state estimation of the linear static Kalman filter. In this article, state x represents the inductance current in *LCL* filter. The Kalman filter can be expressed as $\hat{x}[k+1|k] = A_d\hat{x}[k|k-1] + B_d u[k] + K(y[k] - C\hat{x}[k|k-1])$. K is the Kalman filter gain, $K = A_d P[k|k-1]C^T(CP[k|k-1]C^T + R)^{-1}$, $P[k|k] = P[k|k-1] - KCP[k|k-1]$. In normal conditions, the probability density function of the calculated residual takes the following form $\gamma \sim N(E(\gamma), \sigma_\gamma)$, where $E(\gamma)$ is expectation of the calculated residual and σ_γ is the standard error. With the SSD, γ is denoted as

$$\gamma \sim N(E(\gamma) + \gamma_{at}, \sigma + \sigma_{at}) \tag{1}$$

where γ_{at} is the bias generated by SSD and σ_{at} is the variation in standard error. The residual γ distribution does not follow the distribution in normal conditions. In the conventional detection method, a threshold γ_t is set to detect residual γ variation. When $\gamma > \gamma_t$, the SSD is detected. But a constant threshold may lead to a malfunction. To enhance cybersecurity, an adaptive CUSUM chart is proposed to monitor the standard error shift of the residual γ, which is expressed as follows:

$$U_i = \max(0, U_{i-1} + \sigma_{\gamma i} - E(\sigma_\gamma) - T), i > 1 \tag{2}$$

$$T = \begin{cases} \frac{(U_i - \sigma_{\gamma i}) + (1-\lambda)s}{U_i - \sigma_{\gamma i}}, & if\ (U_i - \sigma_{\gamma i}) < -s \\ \lambda, & if\ |(U_i - \sigma)| < s \\ \frac{(U_i - \sigma_{\gamma i}) - (1-\lambda)s}{U_i - \sigma_{\gamma i}}, & if\ (U_i - \sigma_{\gamma i}) > s \end{cases} \tag{3}$$

where U_i is cumulative sum, $U_1 = 0$; $\sigma_{\gamma i}$ is the standard error in the i_{th} window. $E(\sigma_\gamma)$ is the expectation of the residual standard error in normal conditions which is calculated experimentally. T is determined by $U_i, \sigma_{\gamma i}, \lambda$, and s using Huber function [7]. Based on the recommendation for CUSUM design in [8], the threshold values can be set as $nE(\sigma_\gamma)$, n=0.25,0.5,1,1.5.... According to (2), s is used to quantify the standard error shift. Considering the impact of noise and parameter uncertainties, $s = 1.5E(\sigma_\gamma)$ is used as recommended for CUSUM design. Thus, when the $|(U_{i-1} - \sigma)|$ is great than $1.5E(\sigma_\gamma)$, an adaptive threshold will be implemented in this article. According to the table given by Hawkins (1993a) [8], $\lambda = 0.25E(\sigma_\gamma)$ is used in the adaptive CUSUM chart to detect the moderate size shift of the standard error, which also determines the predefined threshold as shown in Fig. 1(b). Once the $\sigma_{\gamma i}$ increases rapidly and crosses the predefined threshold, the T will be changed, and the corresponding threshold decreases, which makes the detection algorithm more sensitive to SSD. The value of s and λ can be further optimized in the experiment.

The following summarizes the parameter selection for the adaptive CUSUM chart: 1) develop a Kalman filter for state estimation in a grid-connected inverter; 2) conduct a testing experiment in a grid-connected inverter and calculate residual between estimation and measurement; 3) calculate the expectation of standard error $E(\sigma_\gamma)$; 4) determine the values of s and λ based on $E(\sigma_\gamma)$ and discussion provided in the previous paragraph; 5) tune the parameters s and λ until all testing scenarios are validated in the experiment.

Fig. 1(b) shows the flowchart for SSD detection. To achieve fast intrusion detection, the proposed method detects SSD when $U_i > 0$. Fig. 2 shows the performance of a conventional CUSUM and an adaptive CUSUM chart under time-varying standard error. The anomaly appears at 0.15 s. In Fig. 2(a), because of various standard error, U_i restores to zero around 0.21 s which is a false alert. With adaptive T, the adaptive CUSUM

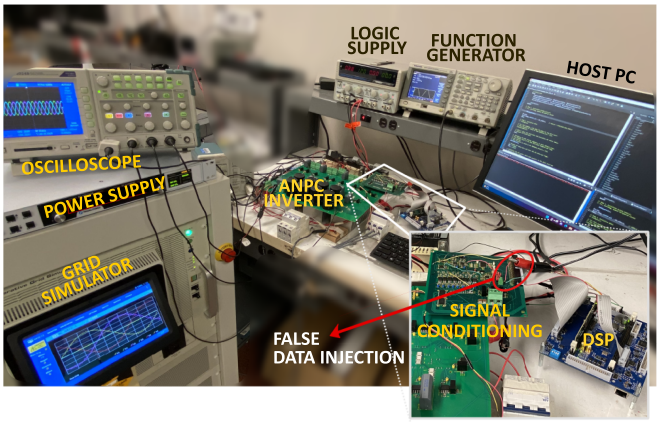

Fig. 3. Experiment setup for the detection method verification.

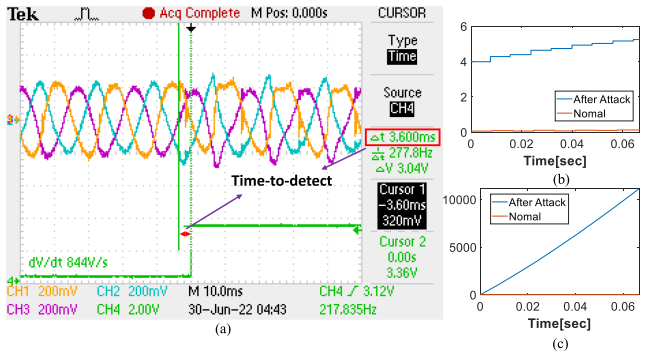

Fig. 4. (a) Three-phase output current in the ANPC inverter and detection time, where the green line represents the detection result, blue, yellow, and pink line are three-phase current, respectively. (b) Standard error of γ. (c) Cumulative sum of the standard error.

chart shows better detection robustness, as shown in Fig. 2(b) ($t > 0.15\,s, U_i > 0$).

III. Experimental Results

To validate the proposed SSD detection method, a hardware experiment is set up as shown in Fig. 3 using an active neutral point clamped (ANPC) inverter. The inverter parameters are: $L = 0.5\,mH$, $r_L = 0.67\,\Omega$, $C_f = 3.9\,\mu F$, and $L_g = 4.5\,mH$, which are also considered for the Kalman filter design.

A. Case Studies

1) Scenario 1: In this scenario, an SSD ($\beta = sin(2\pi t)$) is low-frequency data that is injected into the measured inductance current. Fig. 4(a) shows the disturbance of the output current due to the SSD. The standard errors of the calculated residual γ are shown in Fig. 4(b). Compared to the normal condition, the standard error increased after the breach. In addition, the standard error accumulates and increases rapidly as shown in Fig. 4(c). The detection time (3.6 ms) is shown in Fig. 4(a). The time-to-detect of the conventional method is 15.7 ms. Thus, the comparative result of two methods validates the proposed method in SSD detection.

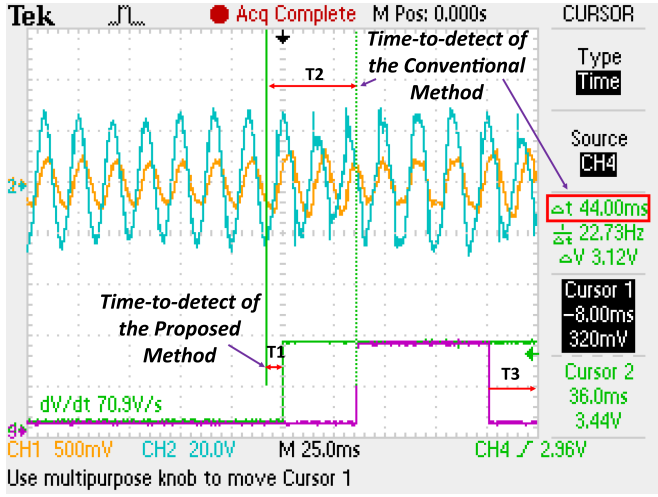

Fig. 5. Comparison result between the conventional detection and the proposed method, where the yellow line represents the phase-A output current in the ANPC inverter, the blue line is the phase-A capacitor voltage in the filter, the green line is the detection result of the proposed method, the pink line is the detection result of the proposed method.

2) Scenario 2: In the second scenario, the performance comparison between the proposed method and a conventional method described in Section II-B is studied. An SSD ($\beta = 0.5sin(10\pi t)$) is injected into inductance current measurements. As shown in Fig. 5, the distortion appears in the output current after this attack. The proposed method detects the SSD using 5.5 ms. Compared to the proposed method, the conventional detection method takes 44 ms to identify this attack using a constant threshold γ_t. Additionally, the conventional method stops alarming during T3. Because the calculated residual γ varies periodically. The constant threshold cannot detect SSD when the magnitude of γ is smaller than the constant threshold γ_t. Therefore, the proposed method is more robust in SSD detection.

B. Comprehensive Analysis and Evaluation

This section analytically demonstrates the robustness of the proposed method under different noise covariance matrices and low-frequency SSD. The performance of the Kalman filter-based estimation method depends on the accurate modeling of the noise and uncertainties in the controller and measurement. A mismatch between the noise covariance matrices, i.e., Q process noise covariance and R measurement noise covariance matrices, in Kalman filter design and uncertainties in the hardware may lead to a degraded estimation performance. To obtain an optimal observer gain K, different noise covariance matrices were implemented in the simulation before the hardware experiment. Fig. 6(a) shows that a histogram plot of the calculated residual γ in the output current estimation using four different R, Q. As shown in Fig. 6(a), the Kalman filter using $R_5Q_{0.1}$ performs better with the γ groups being around zero. Using $R_1Q_{0.1}$, the histogram indicates a constant estimation error (-0.25) in the estimation result. Compared to $R_5Q_{0.1}$, there is a larger residual variation in the estimation result using $R_1Q_{0.5}$ and

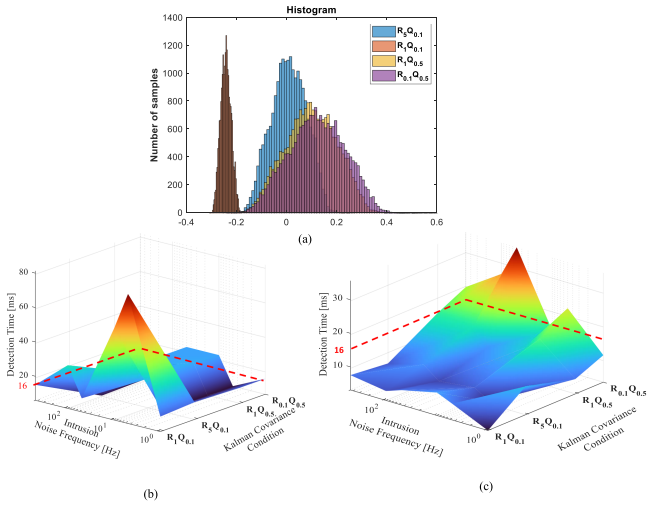

Fig. 6. (a) Histogram of the calculated residual γ under different noise covariance matrices. (b) 3-D plot illustrating the conventional detection method sensitivity to intrusion noise frequency and noise covariance matrix in Kalman filter. (c) 3-D plot illustrating the proposed detection method sensitivity to intrusion noise frequency and noise covariance matrix in Kalman filter (where $R_m Q_n$ represents the noise covariance matrix in measurement and controller, respectively, m, n is diagonal elements in the covariance matrix).

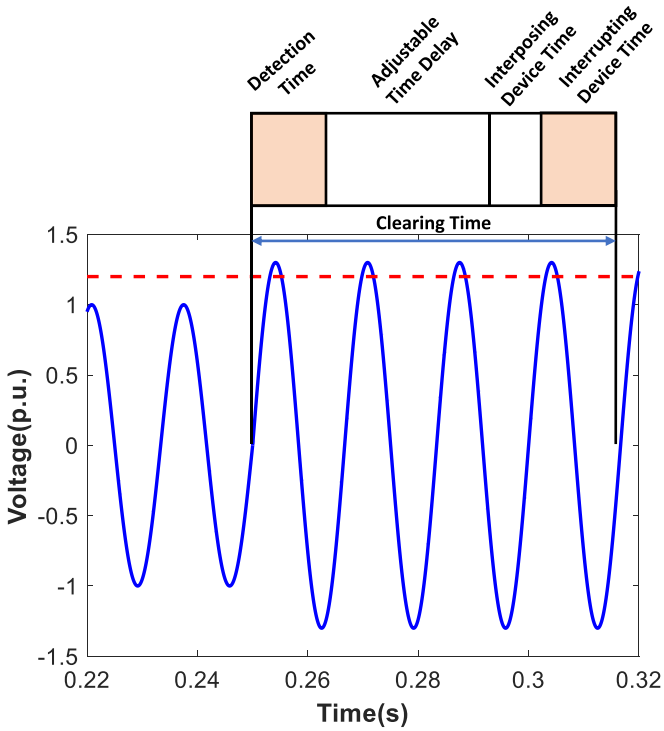

Fig. 7. Clearing time definition in IEEE Standard 1547.

$R_{0.1}Q_{0.5}$. Experimental results in Fig. 6(b) also demonstrate that the proposed method using $R_5Q_{0.1}$ is more efficient in the detection.

To evaluate the proposed detection method, different noise covariance matrices and SSD frequencies (1–500 Hz) were implemented in the hardware testbed. The detection time for different SSD of the conventional and the proposed method are shown in Fig. 6(b) and (c). The results indicate a longer time to detect ($> 16\,ms$, one cycle at 60 Hz) in the conventional method. And the detection time of the conventional method is around 24 ms when SSD with low frequency. When $R > Q$, such as $R_1Q_{0.1}$, $R_1Q_{0.5}$ and $R_5Q_{0.1}$, the detection time of the proposed method is less than 16 ms in Fig. 6(c). This result not only corroborates the results of the simulation analysis in Fig. 6(a), but also demonstrates the robustness of the proposed method in SSD detection when rational noise covariance matrices are used.

C. Time-to-Detect Discussion

We want to clarify some guidelines listed in the IEEE Standard 1547 [6], 1547.3 [9], and 1547.1-2022 [10]. IEEE Standard 1547 is the fundamental standard that specifies a set of uniform requirements for the interconnection of DER with the electric power system. IEEE Standard 1547.3 is a guideline for monitoring, information exchange, and control of distributed resources interconnected with power systems, but it focuses on the interconnection of the information path to power grids and does not address SSD. IEEE Standard 1547.1-2022 provides testing and evaluation procedures, including the recommended time to detect for abnormal voltage and frequency operation. According to Fig. 7 provided by this standard, the detection time is often 8–16 ms, which is the minimum length of time from the inception of the abnormal condition to the change in the state of the inverter's output. As we consider SSD as one type of anomaly, the experimental results in Section III-B show that the corresponding time-to-detect using our proposed detection method is less than 16 ms, which meets the requirement in IEEE Standard 1547 and has superior performance than the existing conventional methodologies.

IV. Conclusion

This letter presented a Kalman filter-based SSD detection method for the grid-connected inverter. A residual between the control reference and the estimation was analyzed from a statistical perspective. An adaptive CUSUM chart was used to monitor the standard error shift of the residual. The hardware experiment validated the proposed method. In addition, a comparison experiment demonstrated that the proposed method performed better than a conventional method. Finally, an evaluation experiment was conducted to verify the feasibility of the proposed method under different noise covariance matrices.

References

[1] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters–Challenges and vulnerabilities," *IEEE Trans. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5326–5340, Oct. 2021, doi 10.1109/JESTPE.2019.2953480.

[2] A. Barua and M. A. A. Faruque, "Hall spoofing: A non-invasive DoS attack on grid-tied solar inverter," in *Proc. 29th USENIX Secur. Symp.*, 2020, pp. 1273–1290. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/barua

[3] J. Selvaraj, G. Y. Dayanıklı, N. P. Gaunkar, D. Ware, R. M. Gerdes, and M. Mina, "Electromagnetic induction attacks against embedded systems," in *Proc. Asia Conf. Comput. Commun. Secur.*, 2018, pp. 499–510.

[4] N. R. Gajanur, M. D. Greidanus, S. K. Mazumder, and M. A. Abbaszada, "Impact and mitigation of high-frequency side-channel noise intrusion on the low-frequency performance of an inverter," *IEEE Trans. Power Electron.*, vol. 37, no. 10, pp. 11481–11485, Oct. 2022, doi 10.1109/TPEL.2022.3170885.

[5] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Trans. Ind. Inform.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017.

[6] *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources With Associated Electric Power Systems Interfaces*, IEEE Standard 1547-2018 (Revision of IEEE Std 1547-2003), 2018.

[7] M. Riaz, B. Zaman, I. A. Raji, M. H. Omar, R. Mehmood, and N. Abbas, "An adaptive EWMA control chart based on principal component method to monitor process mean vector," *Mathematics*, vol. 10, no. 12, 2022, Art. no. 2025.

[8] D. C. Montgomery, *Introduction to Statistical Quality Control*. Hoboken, NJ, USA: Wiley, 2020.

[9] *IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected With Electric Power Systems*, IEEE Standard 1547.3-2007, 2007.

[10] *IEEE Standard Conformance Test Procedures for Equipment Interconnecting Distributed Energy Resources With Electric Power Systems and Associated Interfaces*, IEEE Standard 1547.1-2020, 2020.