
Article:
Jamali, M., Sadabadi, M.S., Davari, M. et al. (2025) Resilient-by-design control for in situ primary controller of grid-following inverter-based resources by a novel state augmentation to tolerate false data injection cyberattacks. IEEE Transactions on Power Electronics, 40 (2). pp. 2746-2760. ISSN: 0885-8993

https://doi.org/10.1109/tpel.2024.3465467

Resilient-by-Design Control for in Situ Primary Controller of Grid-Following Inverter-Based Resources by A Novel State Augmentation to Tolerate False Data Injection Cyberattacks

Mahmood Jamali, Mahdieh S. Sadabadi, *Senior Member, IEEE*, Masoud Davari*, *Senior Member, IEEE*, Subham Sahoo, *Senior Member, IEEE*, and Frede Blaabjerg, *Fellow, IEEE*

***Abstract*—With the increasing number of three-phase grid-following (GFL) inverter-based resources (IBRs) in modern power grids deploying cyber-physical systems, they are required to possess more intelligence with diverse functionality and communication capabilities. However, the cyber threats of smart inverters are omnipresent due to the immense usage of data and communication devices. This paper proposes a novel resilient vector current control strategy for GFL IBRs to alleviate the destructive impacts of false data injection (FDI) attacks while ensuring the stability and desired performance of GFL IBRs. Even with proper upper-layer control mechanisms in place, attackers can exploit vulnerabilities in GFL IBR's primary control, specifically "*inverter output controller*." In such cases, FDI attacks can manipulate the control commands sent to the pulse width modulator, thereby adversely impacting the quality of the output power. To this end, auxiliary control states are augmented and incorporated into the state feedback controller of GFL IBRs, thus enhancing resilient performance against FDI attacks. Theoretical analysis using Lyapunov theory and matrix properties rigorously supports the proof of stability and extends control design considerations. Comparative simulations and experimental results illustrate the resilience and effective functionality of the proposed control scheme.**

The work of Masoud Davari was supported in part by the Division of Electrical, Communications and Cyber Systems (ECCS) in the U.S. National Science Foundation (U.S. NSF) through the core program of Energy, Power, Control, and Networks (EPCN) under ECCS-EPCN-EAGER Award #2405252, ECCS-EPCN Award #1902787, and ECCS-EPCN Award #1808279 and by the Office of International Science and Engineering (OISE) in the U.S. NSF through the International Research Experiences for Students (IRES) program under OISE-IRES Award #2152905; in part by the dSPACE company; in part by the Verivolt company; in part by the Semikron Danfoss company; in part by the Professional Development Part of Masoud Davari's Discovery & Innovation Award from the 2020–2021 University Awards of Excellence at Georgia Southern University; and in part by the 2022 Impact Area Accelerator Grant funded by Georgia Southern University—where all the experiments to test the effectiveness of the proposed method were conducted in the Laboratory for Advanced Power and Energy Systems (LAPES). *(*Corresponding author: Masoud Davari.)*

Mahmood Jamali is with the Department of Automatic Control and Systems Engineering, University of Sheffield, Sheffield S1 3JD, United Kingdom (e-mail: mahmood.jamali@sheffield.ac.uk).

Mahdieh S. Sadabadi is with the Department of Electrical and Electronic Engineering, University of Manchester, Manchester, United Kingdom (e-mail: mahdieh.sadabadi@manchester.ac.uk).

Masoud Davari is with the Department of Electrical and Computer Engineering, Georgia Southern University (Statesboro Campus), Statesboro, GA 30460 USA (e-mail: mdavari@georgiasouthern.edu; davari@ualberta.ca).

Subham Sahoo and Frede Blaabjerg are with AAU Energy (Department of Energy), Aalborg University, Aalborg 9220, Denmark (e-mails: sssa@energy.aau.dk; fbl@energy.aau.dk).

***Index Terms*—Cyber-physical systems (CPSs), false data injection (FDI), resilient vector current control schemes, three-phase grid-following (GFL) inverter-based resources (IBRs).**

I. Introduction

Due to the ever-increasing demand for electrical energy, concerns regarding global warming, and the depletion of traditional energy sources such as fossil fuels, conventional power networks are transitioning towards modern power grids. This transition involves the integration of distributed generation units, renewable energy resources, battery storage systems, and plug-in electric vehicles [1]. Grid-following (GFL) inverter-based resources (IBRs) play a vital role in facilitating this transition, as they are employed to be an interface between new power generation technologies and electrical power grids. Smart three-phase GFL IBRs (hereinafter called GFL IBRs for ease of reference) make the overall power systems more flexible and provide additional capabilities such as power quality improvement [2]. Hence, sophisticated control mechanisms are imperative in modern power grids to enhance the resilience of operation, efficiency, and effective control of GFL IBRs that are "smarter." Integrating traditional power systems, acting as the central entity with information technologies, leads to utilizing cyber-physical systems (CPSs) [3].

The efficient operation of CPS-based microgrids and modern grids hugely relies on the collection, processing, and transmission of information. Although the accumulation of information and communication technologies is expected to enhance the resilience of electrical power systems against contingencies, it also exposes the entire system, including individual devices like smart IBRs, to be highly vulnerable to any cyber threat, including network attacks and device-level attacks. This paper concentrates on attacks arising from firmware updates through the CPS. These updates are a critical component of communication technologies, as they play a substantial role in maintaining the security, functionality, and performance of various devices and systems [4], [5]. Adversaries exploit this by attempting to maliciously manipulate power system operations, potentially causing blackouts, equipment damage, cascaded failure, and so forth. One notable example of cyber-attacks in power systems was carried out by the *Sandworm*

attack group in Ukraine, which paralyzed the power supply for thousands of consumers [6].

Recent studies have pointed out some resilient-related issues and attack identification challenges in CPS-based microgrids and modern grids; see [5], [7]–[10] and references therein. The authors of [11] suggest a detection method based on dynamic watermarking for a grid-tied inverter to identify any cyber-attack targeting sensor measurements. Similarly, the research in [12] proposes an active defensive mechanism for grid-tied photovoltaic systems. Therein, the watermarking technique is employed to detect any adversarial manipulation of voltage/current sensor readings.

However, these detection methods may not be efficacious if the intelligent adversary is capable of avoiding detection from the attack identification tools. This matter inevitably necessitates investigating mitigation control schemes for smart inverters in CPS-based microgrids and modern grids. From a control perspective, the development of resilient control techniques for GFL IBRs in CPS-based microgrids and modern grids is demanding since their response must be quick—typically within a time duration ranging from 0.5 to 5 ms—which is provided by IEEE Std 1547.P10-2018 [13]. This matter means that actions to cyber-attacks must be swift to avert undesirable effects and unpredictable consequences.

The leading research on modern power networks' cyber-resilient control and mitigation strategies centers around islanded microgrids. The reader is referred to the latest research and studies discussing this subject in [14], [15]. In these papers, the ultimate control objective is to design a system-level resilient controller in the secondary control layer of the islanded microgrids to mitigate the adverse consequences of cyber-attacks, particularly false data injection (FDI).

In the domain of CPSs, FDI attacks can appear in various locations within closed-loop control systems, including sensors and actuators. Control input attacks, which intentionally manipulate control signals away from their intended values, are able to disrupt the control law potentially [16]. Although such attacks may seem commonplace, they involve a scenario where an attacker stealthy infuses some false data into the control input channels to render the control commands incorrect [17]. Detecting FDI attacks can be challenging, especially if attackers manipulate data subtly. As already witnessed in numerous real-world examples, the occurrence of FDI attacks in modern power grids poses a critical threat since it can potentially trigger broad-scale blackouts, and lead to substantial economic losses, all of which can have far-reaching consequences [18]. In general, lessons learned from real-world cyber-attack-made incidents in the power grid domain show that firmware malware attacks can directly target inverters.

As discussed in [5], [19], [20], different devices' primary controls in both operation modes of CPS-based microgrids and modern grids are still in danger of being targeted by malicious adversaries through firmware updates. Some of these layers are more vulnerable and can be easily attacked by cyber threats. Considering this matter, it is essential to recognize that even with upper-layer modifications, the control commands and/or measurements at the device level of GFL IBRs may still be scrutinized or scanned by the attackers through firmware updates. Intelligent attackers may choose to either physically perform to disrupt the operation of hardware components such as digital signal processors (DSPs) and cause false readings or engage in firmware replacement to alter the device configuration [21].

Furthermore, devices installed in the field may require regular updates to address bugs and/or introduce new features. Typically, updating the firmware of inverters involves using specialized procedures and protocols designed for the specific inverter model. The process can vary depending on the manufacturer and the type of inverter—e.g., see [22], [23]. Still, here are some common methods used for firmware updates. Many modern inverters support remote firmware updates, where new firmware is downloaded and installed over the internet or through dedicated communication protocols defined in the IEEE 1547-2018 standard (e.g., SunSpec Modbus) [13]. This approach allows for convenient updates without the need for physical access to the inverter. In some cases, firmware updates may be delivered and installed automatically through local cloud-based platforms or even universal serial bus (USB) keys [24]. In all the ways mentioned above, IBRs become more interconnected with other components and are often linked to external networks for firmware updates. This connectivity increases the attack surface, offering more opportunities to exploit vulnerabilities.

Cyberattacks targeting the firmware on grid-connected smart inverters are a genuine concern due to their potential impact on the stability and security of electrical power grids. These vulnerabilities could exist due to coding errors, insecure protocols, or outdated software components. As highlighted in survey papers [21], [25], [26], malicious actors can inject malware into the firmware of smart inverters. Attackers could intercept legitimate firmware updates being sent to smart inverters and replace them with malicious versions. This malware can alter not only the acquisition gain of internal sensors but also control commands and parameters. By tampering with the firmware, an adversary can utilize various techniques to extract valuable information, including sensor measurements and pulse width modulation (PWM) references, and execute FDI attacks to compromise the integrity of control commands, as detailed in [27]–[30]. This type of attacker possesses the capability to modify the data transmitted to microcontroller units that are programmed in the firmware saved in the external memory, ultimately resulting in erroneous inverter operation [21]; see Fig. 1. Therefore, by placing great emphasis on securing individual devices, the entire power system becomes less vulnerable to coordinated cyber-attacks.

In the grid-following operation mode, the frequency and the voltage at the point of common coupling (PCC) are dominantly dictated by the upstream grid. It is noteworthy that this paper exclusively focuses on the FDI-resilient-by-design control of the so-called "*inverter output controller*" among GFL IBR's primary control, which comprises two stages, i.e., power-sharing controller and inverter output controller, to ensure the delivery of the power amounts demanded into the PCC; see [31] and the references therein. In other words, this article considers the primary control stage that should control and regulate the output currents consisting of an inner loop for

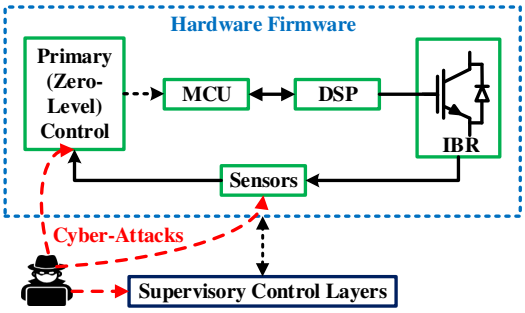

Fig. 1. Visualization of cyber-attacks impacting on the primary and supervisory control layers of an IBR showing microcontroller unit (MCU), and digital signal processor (DSP).

the current regulation (also known as zero-level or device-level control) [5], [31]. For ease of reference, that stage is hereinafter called "*primary control*."

As a result, FDI attacks can substantially impact direct-quadrature (dq)-frame signals on control channels of pulse width modulators. The accuracy of such control commands is crucial as any error or corruption of them will mislead into incorrect switching sequences. Thus, this research presents a control framework to ensure that the switching and modulation are performed correctly. To this end, auxiliary control dynamics are augmented to the conventional state feedback controller for enhancing the resilient feature and ensuring stability in the presence of data integrity cyber-attacks. While the study in [5] has addressed the challenges of control design for GFL IBRs in the presence of faulty sensors, their methodologies fall short in scenarios where attackers manipulate data coming from the controller. To the best of the authors' knowledge, no resilient and robust controls have been specifically designed for the primary control of GFL IBRs under FDI attacks. The key contributions of this paper are summarized as follows.

1) It proposes a novel primary control for GFL IBRs by a novel state augmentation mechanism introduced in this research study, ensuring accurate pulse modulation and switching while maintaining system stability even in the presence of FDI cyber-attacks.
2) It synthesizes an FDI-resilient-by-design control for GFL IBR's primary control in situ. The proposed controller enhances the resilient performance of GFL IBRs and brings forward an acceptable operation despite FDI attack invasion for GFL IBRs in CPS-based microgrids and modern grids without requiring to rely on attack detection mechanisms and unit elimination processes predominantly. This contribution distinguishes the proposed control scheme from existing mitigation approaches in the literature due to its independence from attack detection protocols. It can ensure the achievement of control objectives even before the attack is identified.
3) It delivers a rigorous stability analysis based on Lyapunov theory that guides engineers through designing control matrices. It is shown that by employing some matrix properties, the outputs tracking errors of GFL IBR equipped with the proposed controller converge to a small neighborhood of zero.
4) The scenario in which the auxiliary dynamics become targeted by the attacker is also addressed. This type of cyber invasion is referred to as "*computational attacks*" [16] in the literature, which aims to distort the control law. Comparative simulations and experimental results certify the proposed control scheme's superiority.

The remainder of the paper is organized as follows. Section II details the mathematical model of a GFL IBR using the LCL filter in the form of state space expression. Section III outlines the proposed control scheme and investigates the close-loop (rigorous) stability. Section IV presents simulation verification, along with the experiments conducted. Section V concludes the paper.

Notation: Throughout this paper, $\mathbf{0}_n$ and $\mathbb{I}_n$ represent an $n\times n$ matrix of zeros and $n \times n$ identity matrix, respectively. $\|.\|$ denotes the standard 2-norm. $\mathbb{R}+$ represents the set of positive numbers, and $\mathbb{R}^n$ indicates the dimension of a vector with a length of n.

II. Mathematical Model of GFL IBRs

Referring to Fig. 2, the dynamic model of GFL IBRs (outfitted) with an LCL filter can be described in the form of state space equations in the dq reference frame as follows.

$$\dot{x} = Ax + Bu \tag{1a}$$
$$y = Cx \tag{1b}$$

where $x = [i_{1d} \;\; i_{1q} \;\; i_{2d} \;\; i_{2q} \;\; v_{cfd} \;\; v_{cfq}]^T \in \mathbb{R}^6$ is the state vector, the input vector is stated as $u = [m_d \;\; m_q]^T \in \mathbb{R}^2$, the output vector is described as $y = [i_{2d} \;\; i_{2q}]^T \in \mathbb{R}^2$, and

$$A = \begin{bmatrix} -\frac{R_{t_1}}{L_{f_1}} & \omega & \frac{R_f}{L_{f_1}} & 0 & -\frac{1}{L_{f_1}} & 0 \\ -\omega & \frac{R_{t_1}}{L_{f_1}} & 0 & \frac{R_f}{L_{f_1}} & 0 & -\frac{1}{L_{f_1}} \\ \frac{R_f}{L_{f_2}} & 0 & -\frac{R_{t_2}}{L_{f_2}} & \omega & \frac{1}{L_{f_2}} & 0 \\ 0 & \frac{R_f}{L_{f_1}} & -\omega & \frac{R_{t_2}}{L_{f_2}} & 0 & \frac{1}{L_{f_2}} \\ \frac{1}{C_f} & 0 & -\frac{1}{C_f} & 0 & 0 & \omega \\ 0 & \frac{1}{C_f} & 0 & -\frac{1}{C_f} & -\omega & 0 \end{bmatrix} \tag{2a}$$

$$B = \begin{bmatrix} \frac{V_{dc}}{2L_{f_1}} & 0 \\ 0 & \frac{V_{dc}}{2L_{f_1}} \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \; C = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \tag{2b}$$

According to Fig. 2, i_{d1} and i_{q1} are the dq elements of the inverter current phasor $\overrightarrow{i_1}$ indicating i_{1a}, i_{1b} and i_{1c}; i_{d2} and i_{q2} are the dq elements of current phasor $\overrightarrow{i_2}$ indicating i_{2a}, i_{2b} and i_{2c}; v_{cfd} and v_{cfq} are the dq elements of RC-filter voltage; m_d and m_q are the modulation indices of the switching for GFL IBR in the dq framework. The state matrices in (1) are expressed in (2).

The parameters of the LCL filter in Fig. 2 are required in (2) and stated as follows: $R_{t_1} \triangleq R_{f_1} + R_f$ and $R_{t_2} \triangleq R_{f_2} + R_f$, L_{f_1}/R_{f_1} are the inductance/resistance corresponding to the IBR side of the LCL filter; L_{f_2}/R_{f_2} are the

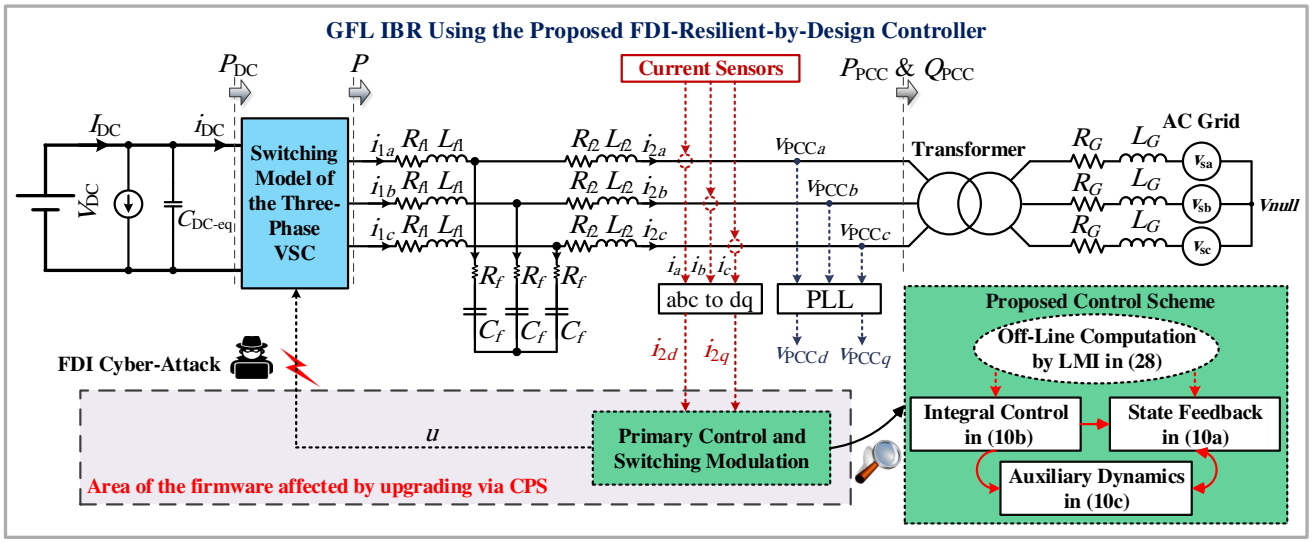

Fig. 2. Detailed block diagram of an LCL-based GFL IBR utilizing the voltage-source converter (indicated as VSC) technology under FDI cyber-attacks manipulating the control input.

inductance/resistance corresponding to the grid side of the LCL filter, and C_f is the shunt capacitance of the LCL filter.

The control input u is employed to guarantee the stability and ensure fast and smooth reference tracking performance, i.e., $i_{2d} \rightarrow i_{2\text{d-ref}}$ and $i_{2q} \rightarrow i_{2\text{q-ref}}$ at the steady-state. Here, $i_{2\text{d-ref}}$ and $i_{2\text{q-ref}}$ are the reference value of i_{2d} and i_{2q}, respectively. Considering the operation of a GFL IBR using the current-controlled technique and PWM, the reference signals, $i_{2\text{d-ref}}$ and $i_{2\text{q-ref}}$, are expressed by $i_{2\text{d-ref}} = \frac{2P_{\text{PCC-ref}}}{3V_{\text{PCCd}}}$ and $i_{2\text{q-ref}} = -\frac{2Q_{\text{PCC-ref}}}{3V_{\text{PCCd}}}$ where $P_{\text{PCC-ref}}$ and $Q_{\text{PCC-ref}}$ denote the desired values for the active power and reactive power injected into the PCC, respectively, and V_{PCCd} represents the d-component of the PCC voltage. Note that $P_{\text{PCC-ref}}$ and $Q_{\text{PCC-ref}}$ are given by a higher-level control system.

GFL IBRs must be equipped with well-designed controllers to meet control objectives, ultimately contributing to grid stability and power quality. Achieving acceptable power quality necessitates minimizing the total harmonic distortion (THD) and keeping the amplitude of three-phase current signals to the required value. Thus, those THD and current amplitude metrics are affected when cyber-attacks are launched. Additionally, if IBRs cannot provide the necessary power, it may result in voltage and frequency deviations on the grid. These deviations can affect the power quality and stability of the overall power grids. Therefore, any instability concerns discussed in this paper pertain to situations in which GFL IBRs are unable to deliver the required active power and reactive power with the standard quality criteria outlined in [13]. Note that this stability criterion is derived from the power system view rather than the control theory standpoint, which typically deals with bounded-input and bounded-output conditions.

A. Data Integrity Cyber-Attack Modeling

Since modern control units are able of remote control authority and firmware updates, these matters increase the vulnerability of control architectures that malicious attackers can exploit. It is worth mentioning that this paper concentrates on cases in which the attack targets the operational technology equipment in the GFL IBR units. In this event caused by such malicious actions, the recovery time can be significantly prolonged [19].

The control channels of PWM generators in GFL IBRs may be vulnerable to cyber-attacks. Consequently, this affects the integrity of the control input u and alters the dynamics described in (1a). Without loss of generality, the dynamics of a GFL IBR equipped with an LCL filter in the presence of FDI attacks on control input channels can be re-expressed as follows.

$$\begin{aligned} \dot{x} &= Ax + B(u + \delta), \\ y &= Cx \end{aligned} \tag{3}$$

where $\delta \in \mathbb{R}^2$ is the FDI attack vector manipulating modulation indices in the primary control of GFL IBRs.

Any data corruption caused by the attacker to manipulate the control commands will generate errors in the switching and modulation process. This interference accordingly hinders GFL IBRs from operating perfectly. Therefore, incorporating attack signals into the dynamics of GFL IBRs in (1a) and developing a resilient control scheme to mitigate the effects of cyber intrusions effectively are crucial. The following section presents a detailed description of the proposed attack-tolerant control scheme. It demonstrates the controller's ability to achieve zero tracking error and ensure the stability of GFL IBRs even in the presence of data integrity actuator attacks.

It is worth notifying that any well-designed control scheme is not entirely resilient against all types of attacks for several fundamental reasons stated in the following. Cyber threats constantly evolve, and new vulnerabilities and attack methods emerge regularly. In other words, cyber attackers tend to be more agile in adjusting their tactics compared to cyber defenders [32]. Note that, as emphasized in [21], the device level of smart inverters is vulnerable to a broad range of cyberattacks—including firmware attacks, and phase-locked loop attacks that aim to compromise smart inverter operational

functions. One noticeable and most probable type of attack through the firmware update is an FDI attack—which can directly affect the performance of GFL IBRs. Moreover, considering the finite resources of controllers and systems, implementing strong security measures often involves trade-offs between performance and cost. While the challenge of designing a controller that is resilient to all types of attacks remains an open question, it is of utmost importance to adopt resilient controllers and proactive security measures across multiple layers to enhance resilience in modern power grids.

Considering this perspective, this paper establishes specific assumptions regarding FDI attacks targeting GFL IBRs. However, the assumptions are realistic and not restrictive. The proposed assumptions cover both time-invariant (constant) and time-varying integrity attack signals that are bounded. However, this research does not consider the case of unbounded attack signals due to the following reasons.

1) As intelligent malicious actors strive to remain undetectable and operate in unintended ways, they typically avoid inserting unbounded signals into control channels to maintain stealthiness. This presumption aligns more closely with real-world settings, as appropriately designed controllers can filter out high-magnitude injections.
2) Additionally, attack identification mechanisms (bad data detectors) easily detect and decline unbounded FDI attacks. Therefore, the following assumption regarding the boundedness of FDI attacks is considered.

Assumption 1. This paper assumes that any FDI attacks injected into the control input channels in (3) are "*uniformly bounded*", i.e., $\|\delta(t)\|$ is finite and that the FDI attacks are externally inserted and independent of the system's states in (1a). Also, it assumes that the attacker can change firmware updates to cause inconspicuous damage.

It is worth mentioning that assuming the boundness of $\|\delta(t)\|$ is without loss of generality as the worst-case cyber-attacks on actuators lead to actuator amplitude saturation in practice.

Remark 1. Note that conducting stability analysis for unbounded cyber-attacks can be mathematically more demanding than for bounded cases. This complexity arises from the diverse forms and intensities that unbounded cyber-attacks can assume. More importantly, sudden and extreme changes in control signals or device behavior are usually easy to detect—but bounded attacks are less likely to raise suspicions. In practical scenarios, attackers often avoid injecting unbounded signals into control commands, particularly given the slow-changing nature of the dq framework.

III. Resilient-by-Design Control Framework

This section introduces a control scheme designed to enhance the resilience of GFL IBRs against FDI attacks, as modeled in Subsection II-A. The proposed control scheme aims to guarantee stability and achieve a fast-tracking performance of the output currents. In other words, it ensures $i_{2d} \to i_{\text{2d-ref}}$ and $i_{2q} \to i_{\text{2q-ref}}$ even in the presence of FDI attacks.

A. Resilient Vector Current Control Scheme Design

A vector current controller in the form of a state feedback controller with an integrator is developed and integrated into the control loop system. Given the open-loop state equation in (1) with state space matrices in (2), the closed-loop system incorporating the state feedback control law and the integral component can be expressed as

$$\dot{x} = (A - BK)x - BK_a x_a \tag{4a}$$

$$\dot{x}_a = -y + r \tag{4b}$$

where $x_a \in \mathbb{R}^2$ represents the state of the integrator, K is the feedback matrix of size 2×6, K_a is a 2×2 integrator gain matrix and $r \in \mathbb{R}^2$ is the reference signal vector. The vector current control scheme in (4) addresses the fast-tracking requirement but lacks sufficient resilience against FDI attacks due to its sensitivity to uncertainties. The following rigorous theoretical analysis demonstrates the limitations of the standard (conventional) state feedback controller in maintaining reference tracking when exposed to FDI integrity attacks.

Let us define $x_{\text{aug}} \triangleq [x^T \ x_a^T]^T$ and $e_{\text{aug}} \triangleq x_{\text{aug}} - [x^{ssT} \ x_a^{ssT}]^T$, where x^{ss} and x_a^{ss} are the steady-state values of x and x_a, respectively. The error vector e_{aug} represents the deviation of the state variables from their steady-state values. The augmented error dynamics of the GFL IBR equipped with the standard feedback controller expressed by (4) in the presence of FDI attack δ is as follows.

$$\dot{e}_{\text{aug}} = A_a e_{\text{aug}} + B_a \delta \tag{5a}$$

$$y_{aug} = C_a e_{\text{aug}} \tag{5b}$$

where

$$A_a = \begin{bmatrix} A - BK & -BK_a \\ -C & \mathbf{0}_2 \end{bmatrix},\ B_a = \begin{bmatrix} B \\ \mathbf{0}_2 \end{bmatrix},\ C_a = \begin{bmatrix} C & \mathbf{0}_2 \end{bmatrix}. \tag{6}$$

Under the principles of linear control systems theory [33], the current error signal y_{aug} can be described as follows.

$$y_{\text{aug}}(t) = C_{\text{a}} \left(e^{A_{\text{a}}} e_{aug}(0) + \int_0^t e^{A_{\text{a}}(t-\tau)} B_{\text{a}} \delta(\tau)\, d\tau \right), \tag{7}$$

where $e_{aug}(0)$ is the initial value of the error vector e_{aug}. The conventional controller is designed so that A_{a} is a Hurwitz (stable) matrix. Let Assumption 1 hold. Given A_{a} as a Hurwitz matrix, there exists an upper bound norm Δ for the FDI integrity attack $\delta(t)$ targeting the GFL IBR such that the following inequality holds [33].

$$\begin{aligned} \|y_{\text{aug}}(t)\| \leq & C_{\text{a}} \left\| e^{A_{\text{a}}} e_{aug}(0) \right\| \\ & + C_{\text{a}} \left\| \int_0^t e^{A_{\text{a}}(t-\tau)} B_{\text{a}} \delta(\tau)\, d\tau \right\| \\ \leq & C_{\text{a}} \left\| \int_0^t e^{A_{\text{a}}(t-\tau)} B_{\text{a}} \delta(\tau)\, d\tau \right\| \end{aligned} \tag{8}$$

Note that, since A_{a} is a stable matrix, $\lim_{t\to\infty} \left\| e^{A_{\text{a}}} e_{aug}(0) \right\| = 0$. Then, according to Assumption 1, one can obtain

$$\begin{aligned} \lim_{t\to\infty} \|y_{\text{aug}}(t)\| &\leq C_{\text{a}} \lim_{t\to\infty} \left\| \int_0^t e^{A_{\text{a}}(t-\tau)} B_{\text{a}} \Delta\, d\tau \right\| \\ &\leq \lim_{t\to\infty} \left\| \int_0^t C_{\text{a}} e^{A_{\text{a}}(t-\tau)} B_{\text{a}}\, d\tau \right\| \|\Delta\| \\ &\leq \left\| C_{\text{a}} A_{\text{a}}^{-1} B_{\text{a}} \right\| \|\Delta\|. \end{aligned} \tag{9}$$

Consequently, using the standard feedback controller, $\left\|C_{\mathrm{a}}{A_{\mathrm{a}}}^{-1}B_{\mathrm{a}}\right\|\|\Delta\|$ remains a non-zero constant, and $\|y_{aug}\|$, which represents the output error, is unable to converge to zero. As a result, this matter prevents error-free tracking of the system's outputs and deficiency of the standard state feedback controller when facing FDI attacks. In the following, auxiliary control dynamics are augmented into the controller to overcome this limitation. This paper shows that such augmentation ensures system stability and enhances the resilience of GFL IBRs under FDI attacks.

The following auxiliary dynamics are developed to attenuate the adverse impacts of cyber-attacks in the stability and current reference tracking; they include the auxiliary states denoted by $z \in \mathbb{R}^2$.

$$\dot{x} = \underbrace{(A - BK)}_{A_r} x - BK_a x_a + \alpha BMz \tag{10a}$$

$$\dot{x}_a = -y + r \tag{10b}$$

$$\dot{z} = -Fz - \alpha(D_1 x - D_2 x_a). \tag{10c}$$

where (10), M and $D = [D_1 \;\; D_2]$ are interconnection matrices with sizes of 2×2 and 2×8, respectively; F represents a 2×2 symmetric positive definite matrix; and $\alpha \in \mathbb{R}_+$ is a control gain to be determined. Note that the auxiliary states z may be accessible to adversaries. However, simulations will later show that the proposed control scheme is also resilient against FDI attacks targeting the dynamics in (10c). The following result shows that the interconnected system in (10) in the absence of cyber-attacks is asymptotically stable. Most importantly, including augmented dynamics does not compromise the system's ability to track the reference values precisely. The dynamics of the closed-loop system in (10) can be rewritten in a new coordinate as follows.

$$\dot{e}_{\text{aug}} = A_a e_{\text{aug}} + \alpha B_a M z \tag{11a}$$

$$\dot{z} = -Fz - \alpha D e_{\text{aug}} \tag{11b}$$

The feedback matrices K and K_a are designed by the operator to ensure the stability of the system described in (10a) and (10b) using several methods such as LQR and Lyapunov methods. Consequently, A_a is chosen to have the system stable. Also, as F is a symmetric positive definite matrix, thus, $-F$ is Hurwitz. As a result, according to Lyapunov theory [34], a symmetric positive definite matrix exists—such as P_1 with an appropriate size—in a way that the following inequalities are held.

$$\begin{aligned} A_a^T P_1 + P_1^T A_a < 0, \\ F^T + F > 0. \end{aligned} \tag{12}$$

To guarantee the stability of the closed-loop dynamics in (6), considering the following substantial design requirement for the interconnection matrices introduced in (10) is crucial.

$$D = M^T B_a^T P_1. \tag{13}$$

The reasoning behind the condition on the interconnection matrices in (13) can be determined by employing Lyapunov stability analysis. By selecting the quadratic-type Lyapunov candidate of

$$V = \alpha e_{\text{aug}}^T P_1 e_{\text{aug}} + \alpha z^T z \tag{14}$$

and taking its time derivative along with the closed-loop dynamics in (6), one can obtain the following expression.

$$\begin{aligned} \dot{V} &= \alpha \left(\dot{e}_{aug}^T P_1 e_{aug} + e_{aug}^T P_1 \dot{e}_{aug} + \dot{z}^T z + z^T \dot{z} \right) \\ &= \alpha e_{\text{aug}}^T (A_a^T P_1 + P_1 A_a) e_{\text{aug}} - \alpha z^T (F^T + F) z \\ &\quad + 2\alpha^2 e_{\text{aug}}^T (P_1 B_a M - D^T) z. \end{aligned} \tag{15}$$

By applying the condition stated in (13) and considering the inequalities in (12), it can be established that the derivative of the proposed Lyapunov function is negative, i.e.,

$$\dot{V} = \alpha e_{\text{aug}}^T (A_a^T P_1 + P_1 A_a) e_{\text{aug}} - \alpha z^T (F^T + F) z < 0. \tag{16}$$

Consequently, the origin of the system in (11) is globally asymptotically stable, thereby implying that output tracks the current references at the steady state. This analysis confirms that the proposed control scheme enables the system to track the desired values in the absence of any cyber intrusions accurately. The following subsection shows that the output signals of the GFL IBR (1b) equipped with the proposed controller in (10) can still track the set-points even in the existence of FDI attacks.

B. Attack-Resilient Analysis

This subsection analyzes the resilience of the proposed control framework in (10) for GFL IBRs in the presence of bounded FDI attacks on the control channel of the PWM generator. In this regard, the 2-norm of the output error at steady-state is utilized as a performance index. This index is denoted as $\lim_{t\to\infty}\|y(t) - r\|$, and it functions as a measure of the system's resilience against data integrity attacks. The results are presented in the following theorem. But before delving into the analysis, it is necessary to introduce some definitions.

Let us express the error term vector as $E = [e_{\text{aug}}^T \;\; z^T]^T$. Note that the steady-state value of the augmented state z is zero. Then, the dynamics of the interconnected system in (11), along with the FDI attack model on the control input, can be written as follows.

$$\dot{E} = A_{\text{cl}} E + B_{\text{cl}} \delta \tag{17a}$$

$$y_{\text{cl}} = C_{\text{cl}} E \tag{17b}$$

The state matrices in (17) are formed in the following manner.

$$A_{\text{cl}} = \begin{bmatrix} A_a & \alpha B_a M \\ -\alpha D & -F \end{bmatrix} \tag{18a}$$

$$B_{\text{cl}} = \begin{bmatrix} B_a \\ \mathbf{0}_2 \end{bmatrix}, \; C_{\text{cl}} = \begin{bmatrix} C & \mathbf{0}_2 & \mathbf{0}_2 \end{bmatrix}. \tag{18b}$$

Theorem 1. *Let Assumption 1 hold, and D is designed based on the condition specified in* (13) *regardless of the specific value assigned to matrix M. As modeled in* (1b) *and outfitted with the proposed controller in* (10)*, the GFL IBR output remains bounded in the presence of bounded FDI attack δ. Moreover, if an adequately large value of α is chosen,*

$\lim_{t\to\infty}(y(t)-r)=[\epsilon_d\ \epsilon_q]^T$, *where* $\epsilon_d\in\mathbb{R}_+$ *and* $\epsilon_q\in\mathbb{R}_+$ *are two sufficiently small non-negative scalars.*

Proof. Based on the principles of linear control system theory, the error state E in equation (17) can be presented as follows.

$$y_{\text{cl}}(t)=C_{\text{cl}}\left(e^{A_{\text{cl}}}E(0)+\int_0^t e^{A_{\text{cl}}(t-\tau)}B_{\text{cl}}\delta\,d\tau\right), \tag{19}$$

where $E(0)$ is the initial value of the state vector E.
Note that since A_{cl} is a Hurwitz matrix, then $\lim_{t\to\infty}\left\|C_{\text{cl}}e^{A_{\text{cl}}t}E(0)\right\|=0$. Given Assumption 1 on the boundedness of the FDI attack δ, one can find a constant vector $\Delta=\sup_{0\le\tau\le t}\|\delta(\tau)\|\in\mathbb{R}^2$ that fulfills the following inequality.

$$\begin{aligned}\|y_{\text{cl}}(t)\|&\le C_{\text{cl}}\left\|\int_0^t e^{A_{\text{cl}}(t-\tau)}B_{\text{cl}}\delta\,d\tau\right\|\\&\le C_{\text{cl}}\left\|\int_0^t e^{A_{\text{cl}}(t-\tau)}B_{\text{cl}}\Delta\,d\tau\right\|.\end{aligned} \tag{20}$$

Therefore, based on the results in [33], the following inequality can be acquired.

$$\begin{aligned}\lim_{t\to\infty}\|y_{\text{cl}}(t)\|&\le\lim_{t\to\infty}\left\|C_{\text{cl}}\int_0^t e^{A_{\text{cl}}(t-\tau)}B_{\text{cl}}\Delta\,d\tau\right\|\\&=\left\|C_{\text{cl}}{A_{\text{cl}}}^{-1}B_{\text{cl}}\Delta\right\|.\end{aligned} \tag{21}$$

Let us define $\mathbf{a}\triangleq(A_a-\alpha^2B_aMF^{-1}D)^{-1}$. In accordance with the Banachiewicz–Schur formula [35], the inverse of A_{cl} is obtained as follows.

$$A_{\text{cl}}^{-1}=\begin{bmatrix}\mathbf{a} & \alpha\,\mathbf{a}B_aMF\\ -\alpha F^{-1}D\mathbf{a} & -F^{-1}-\alpha^2F^{-1}D\mathbf{a}B_aMF^{-1}\end{bmatrix}. \tag{22}$$

By factoring out α^2 and defining $B_aMF^{-1}D\triangleq H$, the matrix $\mathbf{a}$ can be expressed as follows.

$$\mathbf{a}=-\gamma(H-\gamma A_a)^{-1}. \tag{23}$$

where $\gamma=\frac{1}{\alpha^2}$. When α is chosen to have a sufficiently large value, γA_a becomes a bounded and convergent matrix. By virtue of the Neumann series concept [36], the following result is achieved for a sufficiently large value of α. Note that the truncated Neumann series method is utilized to approximate matrix inversion.

$$\gamma(H-\gamma A_a)^{-1}\approx\epsilon\mathbb{I}_8 \tag{24}$$

where $\epsilon\in\mathbb{R}_+$ is a sufficiently small scalar.
The multiplication of ${A_{\text{cl}}}^{-1}B_{\text{cl}}$ and $C_{\text{cl}}{A_{\text{cl}}}^{-1}B_{\text{cl}}$ can be expanded as follows.

$$-{A_{\text{cl}}}^{-1}B_{\text{cl}}=\begin{bmatrix}\mathbb{I}_8\\ -\alpha F^{-1}D\end{bmatrix}\mathbf{a}B_a, \tag{25}$$

and

$$\begin{aligned}-C_{\text{cl}}{A_{\text{cl}}}^{-1}B_{\text{cl}}&=\begin{bmatrix}\mathbf{0}_2 & \mathbb{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2\end{bmatrix}\begin{bmatrix}\mathbb{I}_8\\ -\alpha F^{-1}D\end{bmatrix}\mathbf{a}B_a\\&\approx\epsilon\begin{bmatrix}\mathbf{0}_2 & \mathbb{I}_2 & \mathbf{0}_2 & \mathbf{0}_2\end{bmatrix}B_a\end{aligned} \tag{26}$$

Therefore, considering the above inequality and (24), one can obtain that

$$\lim_{\alpha\to\infty}\left\|-C_{\text{cl}}{A_{\text{cl}}}^{-1}B_{\text{cl}}\right\|\approx\epsilon. \tag{27}$$

As a result of (21) and (27), $\lim_{t\to\infty}\|y_{\text{cl}}(t)\|\le\epsilon$, which implies that each element of $y_{\text{cl}}(t)$ converges to a very small neighborhood of zero at the steady-state for any sufficiently large value of α. Consequently, according to (10b), it can be concluded that $\lim_{t\to\infty}(y(t)-r)=[\epsilon_d\ \epsilon_q]^T$. This part completes the proof. ■

Remark 2. Note that the results given in Theorem 1 are valid for any possible FDI actuator attack that meets the conditions outlined in Assumption 1.

Remark 3. In order to guarantee the safe operation of inverters, they are equipped with protection systems designed to safeguard the inverter and connected equipment from potential disruptive events and faults. For instance, over-current protection is integrated to prevent excessive current from damaging the inverter or connected devices [37]. However, FDI cyber-attacks intend to manipulate the control command of the PWM generator to push the IBR to an undesired operating condition while maintaining stealth. In this case, the signals and commands might remain within permissible limits. Accordingly, the proposed resilient control scheme is implemented to ensure the output signals of the GFL IBR can promptly and accurately restore their reference values while staying connected to the grid and continuing to supply the required power.

IV. Simulations and Experiments

This section presents comparative simulations and experimental results of the proposed resilient vector current control scheme for three scenarios. The first scenario considers FDI attacks on the control inputs of the GFL IBR. In contrast, the second scenario involves FDI attacks on both the control input and computational layer of a GFL IBR. The third scenario explores a situation where FDI attacks on the control inputs of GFL IBRs are intensified in both magnitude and frequency. The fourth one presents the simulation outcomes when the GFL IBR faces random FDI attacks. To assess the efficacy of the controller, the simulations are conducted using MATLAB/Simulink for all scenarios. Moreover, simulation results of the conventional PI controller for GFL IBRs are presented, highlighting its ineffectiveness against FDI attacks. The simulation results for the weak-grid case are also presented and discussed. Lastly, to demonstrate the practicality of the proposed control methodology, the final subsection is dedicated to the experimental results of a GFL IBR. Based on this section's simulations and experiments, the proposed control framework demonstrates the capability to operate effectively in both normal and attack situations. In other words, there is no requirement to update the controller parameters when attacks occur, which prevents unexpected behavior due to the interruptions for tuning control parameters.

The fundamental frequency of the electric power network is 60 Hz, and the nominal voltage is 208 V. Fig. 2, whose parameters are provided in Table I, is considered. The bounded FDI attack, which satisfies Assumption 1, is emulated by the sinusoidal signals corrupting the control commands transmitted to the PWM generator. The interconnection matrices of the control protocol presented in (10) are assigned to be

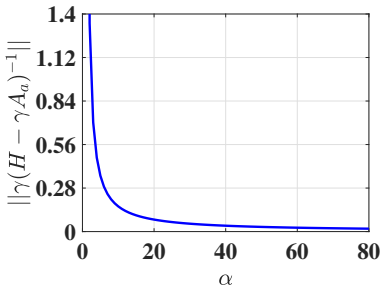

Fig. 3. Norm of the bound in (24) as a function of the control parameter α.

TABLE I
PARAMETERS OF THE GFL IBR UNDER TEST FOR SIMULATIONS AND EXPERIMENTS IN SECTION IV.

Parameter	Value
S_n	10.81 kVA
L_{f_1}/R_{f_1}	1.1 mH/0.01 Ω
L_{f_1}/R_{f_1}	1.1 mH/0.01 Ω
C_f/R_f	15.4 μF/2.08 Ω
$V_{\mathbf{DC}}$	400 V
$f_{\mathbf{sw}}$	8.1 kHz
$f_{\mathbf{grid}}$	60 Hz
$V_{\mathbf{PCC_{rms}}}$	208 V
SCCR (or SCR)	10

$M = 0.15 \times \begin{bmatrix} -1 & 0 \\ 1 & -1 \end{bmatrix}$, $F = \mathbb{I}_2$, and $\alpha = 150$. It is noteworthy that D is selected based on the condition outlined in (13). To determine the value P_1 and state feedback matrix K, it is necessary to solve a linear matrix inequality (LMI) problem using MATLAB [38]. The formulation of the LMI problem is provided by

$$P_1\bar{A}_a^T + \bar{A}P_1 - K^T B_a^T - B_a K + \beta P_1 < 0, \qquad (28)$$

where $\bar{A} = \begin{bmatrix} A & \mathbf{0}_{6\times 2} \\ -C & \mathbf{0}_2 \end{bmatrix}$ and $\beta \in \mathbb{R}_+$. The resilience feature of the proposed control scheme, as described by equation (10), hinges upon the resilience parameter α, where a higher α signifies better resilience against FDI cyberattacks. However, it is essential to note that a tremendous value of α may degrade the transient response characteristics, potentially leading to issues such as overshoot and increased oscillation. Hence, the α value represents a crucial trade-off between transient response performance and resilience enhancement. As presented in Section III, the ultimate error of the output y_{cl} depends on the maximum bound of FDI attacks $||\Delta||$ and the norm $||-\gamma(H-\gamma A_a)^{-1}||$ in (24). Fig. 3 depicts this norm as a function of the control gain α introduced in (10). Increasing the value of α results in a more resilient system—thereby tolerating higher magnitude FDI attacks. In other words, the proposed control law in (10) with a higher value for α can withstand a larger magnitude of FDI attacks while accurately tracking the output current signals to their desired values.

A. Scenario I

This subsection investigates the case in which a malicious actor manipulates the data integrity of the control signals being sent to the PWM generator. The bounded FDI attack signal vector, which emulates the behavior of a possible data integrity attack, is selected to be $\delta = \begin{bmatrix} 2 + 0.2\sin(0.1\ \omega t) & 2.5 + 0.1\sin(0.1\ \omega t) \end{bmatrix}^T$. Note that the attack is launched at t = 2 s and continues until the end of the simulation time. The simulation results for the signals of interest—namely the dq-frame error signals $i_{2d} - i_{\text{2d-ref}}$ and $i_{2q} - i_{\text{2q-ref}}$, three-phase output current i_{abc}, active power P, and reactive power Q of GFL IBR—are displayed in Fig. 4.

First, the initial values for the active power and reactive power are set to be 10 kW and 10 kVAr, respectively. In order to reach the desired active power and reactive power values, load changes suddenly happen at t = 0.5 s and t = 1.5 s, respectively. As shown in Fig. 4, the proposed control scheme is able to mitigate the negative effect of FDI attacks. Second, after the attack occurs, the current signal quickly returns to the desired values within a short period—i.e., less than 0.05 s—and keeps its sinusoidal shape. Fig. 5 depicts the simulation results for the GFL IBR equipped with a conventional PI controller. As observed, the PI controller successfully performs reference tracking before the FDI attack. However, after the cyber-attack, the current, active power, and reactive power signals fail to revert to their nominal values quickly. As a result, the ability to track the references is lost for a considerable time-frame, and the error persists after launching the FDI attack. A notable concern is a significant jump in the three-phase current signal amplitude, which increases from 1 per unit (pu) peak-to-peak to around 6 pu peak-to-peak. This considerable rise could adversely impact the power quality and stability of the overall power grid, potentially leading to the disconnection of the GFL IBR from the grid as the current limit might go over the permissible range.

It is noteworthy that the PI controller's control gains are chosen under the design procedure outlined in [39]. When K_P and K_I are appropriately designed as presented in (29), a zero-pole cancellation leads to a first-order transfer function for the closed-loop system with a time constant of τ—which is typically selected within the range of 0.5 to 5 ms. The time constant considered for the comparison case in Scenario I is 1 ms, which is pretty suitable for VSCs, according to [39].

$$K_P = \frac{L_f}{\tau} \qquad (29a)$$

$$K_I = \frac{R_f}{\tau} \qquad (29b)$$

B. Scenario II

This scenario considers the attacker inserting FDI attacks not only into the control input channel of the PWM generator but also in the augmented control layer presented in (10b). The dynamics of the auxiliary control layer in (11) considering FDI attacks is modified as

$$\dot{z} = -Fz - \alpha De + \bar{\delta} \qquad (30)$$

where $\bar{\delta} \in \mathbb{R}^2$ is the attack vector on the computational layer. It is demonstrated that the proposed control scheme is resilient against such types of FDI attacks where the

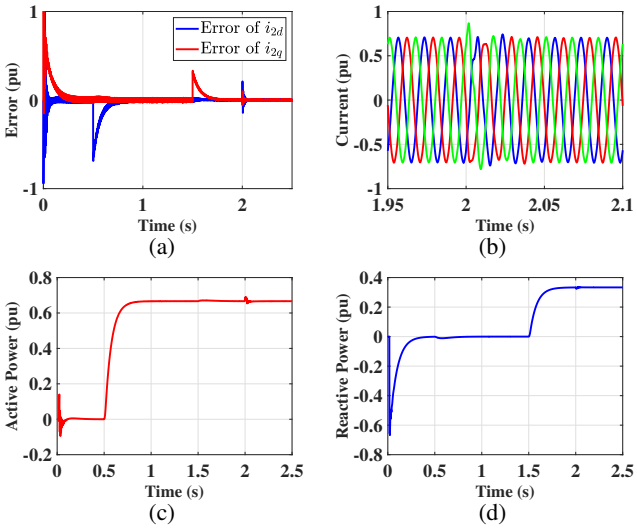

Fig. 4. Performance of the proposed resilient control scheme for *Scenario I*: (a) error between the real value and reference value of i_{2d} and i_{2q}, (b) three-phase current, (c) active power and (d) reactive power of GFL IBR.

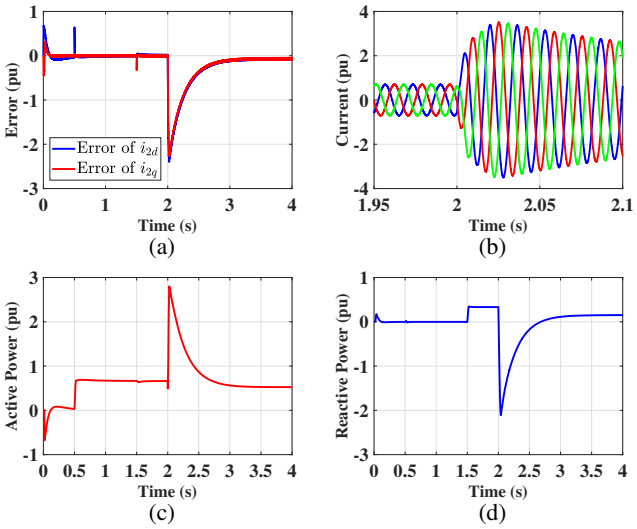

Fig. 5. Performance of the PI controller for *Scenario I*: (a) error between the real value and reference value of i_{2d} and i_{2q}, (b) three-phase current, (c) active power and (d) reactive power of GFL IBR.

attacker aims to alter the control law dictated by the computational layer. The control input channel of GFL IBR is subjected to FDI attacks similar to the previous scenario. The computational FDI attack vector is picked out as $\delta = \begin{bmatrix} 3 + 0.3\sin(0.1\ \omega t) & 3.75 + 0.15\sin(0.1\ \omega t) \end{bmatrix}^T$.

Fig. 6 depicts the simulation outcomes of *Scenario II*. The load change moments are at t = 0.5 s and t = 1 s. Despite of attack occurring at t = 1.5 s on both the control input channel and the auxiliary control dynamic, the proposed control strategy perfectly maintains the stability of GFL IBR. Furthermore, it successfully tracks the desired values of the current signals, thereby resulting in the desired active power and reactive power outputs of GFL IBR.

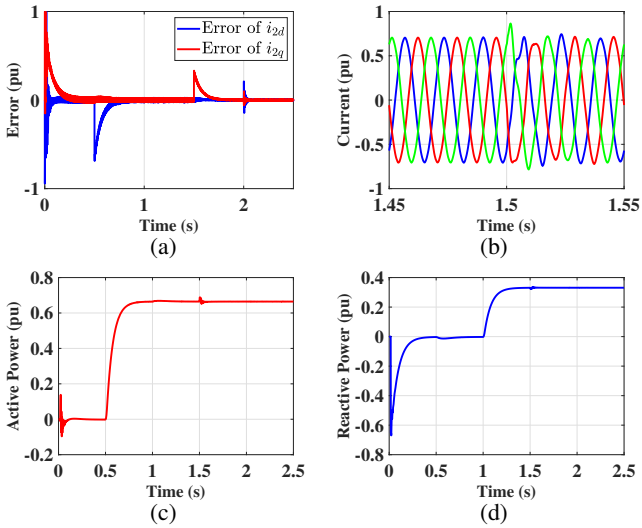

Fig. 6. Performance of the proposed resilient control scheme for *Scenario II*: (a) error between the real value and reference value of i_{2d} and i_{2q}, (b) three-phase current, (c) active power (d) and reactive power of GFL IBR.

C. Scenario III

This scenario considers that a malicious actor launches a more severe FDI attack, both in terms of magnitude and frequency, targeting the control input channel of the GFL IBR. In order to accomplish this, a potential data integrity attack is selected, represented as $\delta = \begin{bmatrix} 4 + 0.5\sin(1100\ \omega t) & 3 + \sin(1000\ \omega t) \end{bmatrix}^T$. The moments of load change and the timing of the attack remain consistent with Scenario I. Figs. 7 and 8 present the simulation results of this scenario for both our proposed control scheme and the conventional PI controller, respectively. As one can observe, the proposed control scheme successfully mitigates the negative impact of severe FDI attacks. After the cyberattack, the signals of interest quickly restore to their nominal values. However, as depicted in Fig. 8, it is apparent that the GFL IBR equipped with the conventional PI controller struggles to recover from severe FDI attacks. This struggle manifests in highly erratic and chattering signals, thus ultimately losing the control system's ability to track reference values accurately. Furthermore, the three-phase current signal deviates from its expected sinusoidal waveform.

It is noteworthy that despite the state feedback controller's effectiveness in rejecting disturbances, as demonstrated in our mathematical analysis (see Subsection III-A), it cannot ensure error-free tracking of the system's outputs when facing severe time-varying FDI attacks on the control input. Additionally, as evident in the simulation results (refer to Fig. 5 and Fig. 8), the conventional PI controller fails to provide rapid recovery after cyberattacks, leading to errors and fluctuations for a significant duration of time.

D. Scenario IV

In this scenario, the GFL IBR integrated with the proposed control scheme is subjected to a bounded but random FDI signal generated by the "Random Number" block in MATLAB/Simulink. The random FDI attack is assumed to

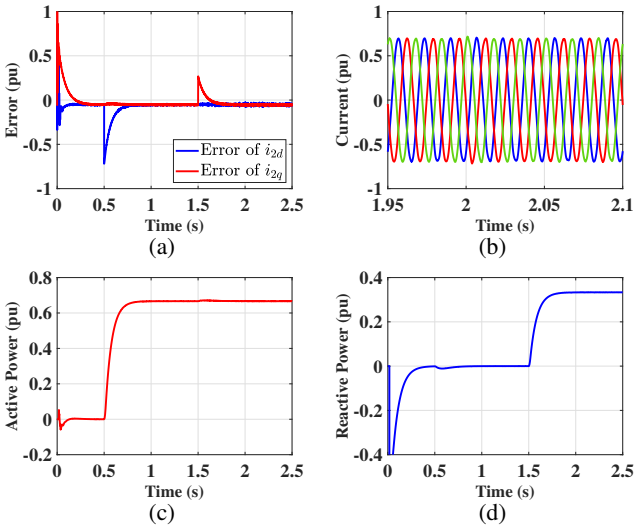

Fig. 7. Performance of the proposed resilient control scheme for *Scenario III*: (a) error between the real value and reference value of i_{2d} and i_{2q}, (b) three-phase current, (c) active power and (d) reactive power of GFL IBR.

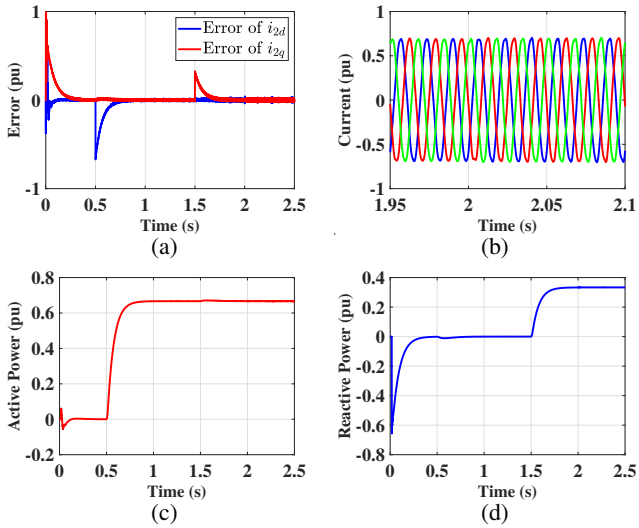

Fig. 9. Performance of the proposed resilient control scheme for *Scenario IV*: (a) the error between the real value and reference value of i_{2d} and i_{2q}, (b) three-phase currents, (c) active power, and (d) reactive power of GFL IBR.

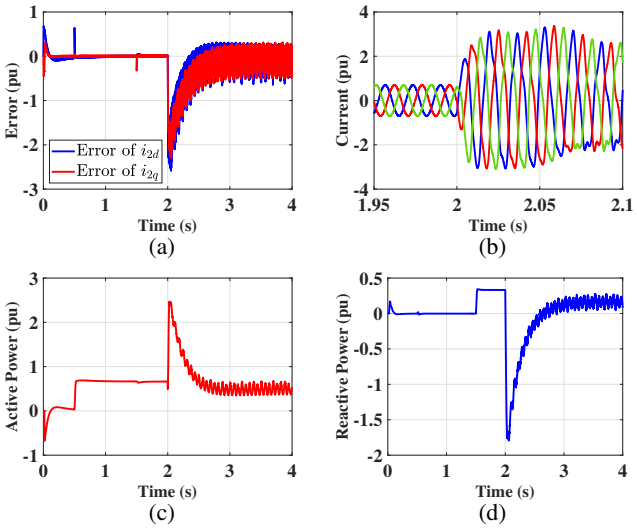

Fig. 8. Performance of the PI controller for *Scenario III*: (a) error between the real value and reference value of i_{2d} and i_{2q}, (b) three-phase current, (c) active power and (d) reactive power of GFL IBR.

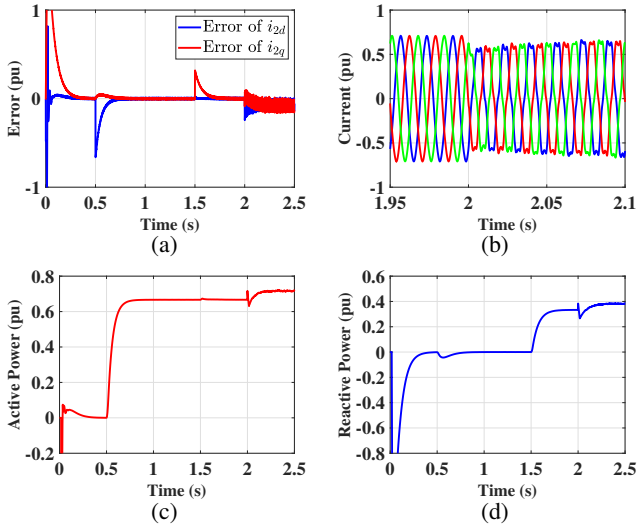

Fig. 10. Performance of the sliding mode controller for *Scenario IV*: (a) the error between the real value and reference value of i_{2d} and i_{2q}, (b) three-phase currents, (c) active power, and (d) reactive power of GFL IBR.

be within the range of -3 to 3. As depicted in Fig. 9, the simulation results demonstrate that even in the presence of random false injections, the proposed control scheme maintains resilient performance, as evidenced by the error-free tracking of the signals of interest. We also test and compare the simulation results for the sliding mode control strategy inspired by [5]. Although this control strategy effectively rectifies sensor faults as claimed by the authors, Fig. 10 shows that it cannot guarantee the desired performance in the presence of FDI attacks on the control command of GFL IBRs. In other words, the sliding mode controller is unable to provide error-free tracking and exhibits a more oscillatory response when the GFL IBR is exposed to FDI attacks on the control command.

E. Scenario V

This subsection addresses weak-grid scenarios for simulation in which the short-circuit capacity ratios (SCCRs or, equivalently, SCRs) are 1.5 and 2, respectively. Multiple factors can influence weak-grid integration, including grid impedance, the type of grid impedance, and the phase-locked loop controller [5], [40]–[43]. It is important to note that the design of a controller for weak-grid integration lies outside the scope of this paper's principles. However, the simulation results are presented to illustrate the performance of the proposed controller when GLF IBR is integrated into weak grids. The load change timings and the FDI attacks remain consistent with Scenario II. As depicted in Fig. 11 and Fig. 12, the proposed control scheme demonstrates its effectiveness

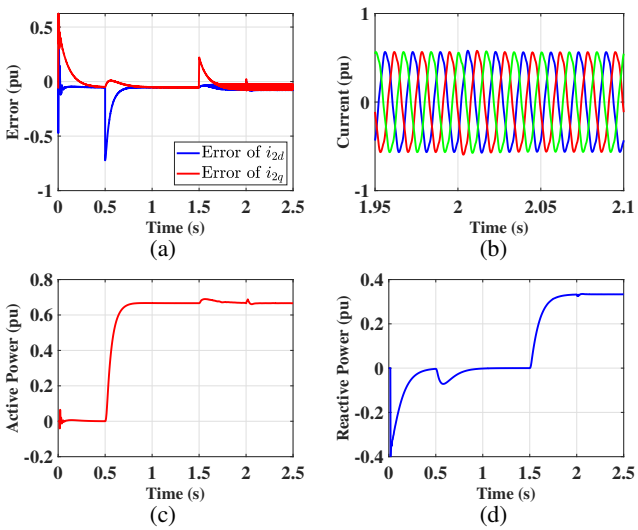

Fig. 11. Performance of the proposed resilient control scheme for *Scenario V* when SCCR = 1.5: (a) error between the real value and reference value of i_{2d} and i_{2q}, (b) three-phase current, (c) active power (d) and reactive power of GFL IBR.

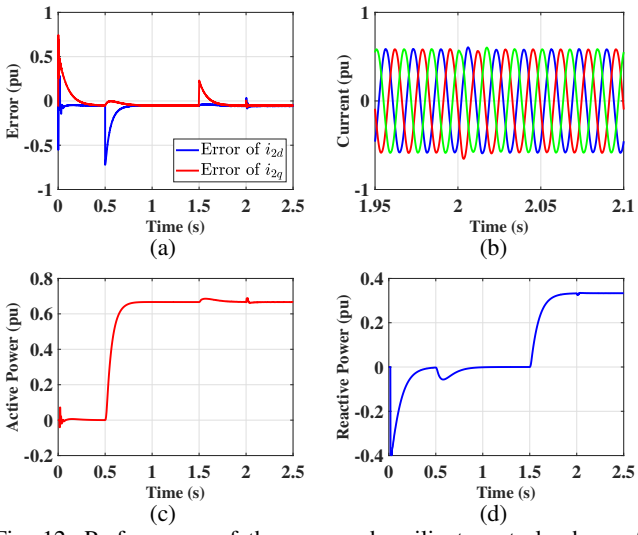

Fig. 12. Performance of the proposed resilient control scheme for *Scenario V* when SCCR = 2 : (a) error between the real value and reference value of i_{2d} and i_{2q}, (b) three-phase current, (c) active power (d) and reactive power of GFL IBR.

even in the condition of weak-grid integration.

F. Experimental Results

The proposed resilient-by-design primary control of GFL IBRs is implemented on a prototype of a GFL IBR unit. Its power modules based on insulated gate bipolar transistors are the Semikron Danfoss "SKM 50 GB 123 D" intelligent power modules. The Semikron Danfoss "SKHI 21A (R)" gate drives and protection circuitry are employed to enable the GFL IBR prototype to function. Additionally, the Verivolt "IsoBlock I-ST-1c"/"IsoBlock V-1c" current/voltage sensors are connected to digital inputs to facilitate the measurement of currents and voltages. The input/output channels of a dSPACE "MicroLabBox (MLBX)" digital real-time controller interface the GFL IBR under test with the measurement and drive circuitry. Furthermore, all the setup parameters employed in

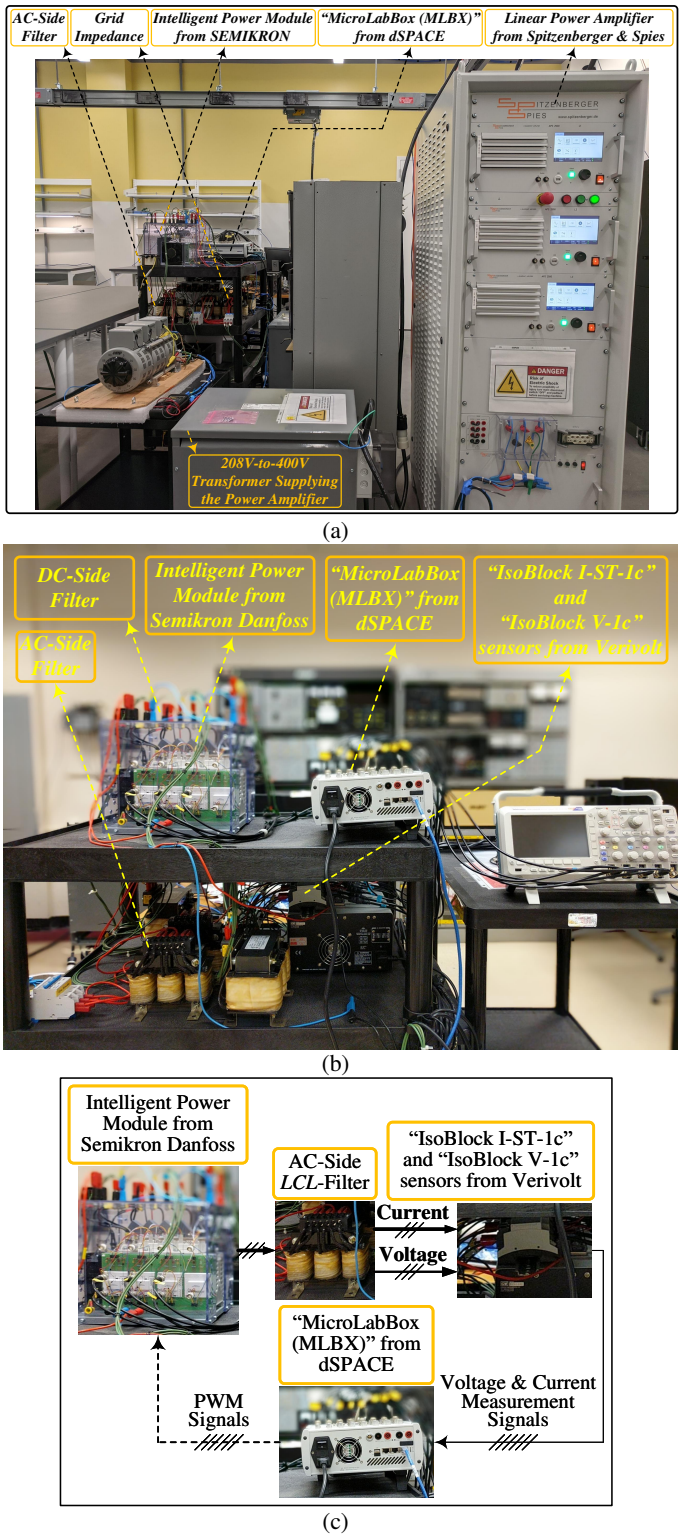

Fig. 13. Test rig deployed to carry out experiments: (a) the complete view and all devices, (b) the details of the GFL IBR under test, and (c) the block diagram of the GFL IBR under test.

the experiments are similar to the simulations, as presented in Table I. In this regard, the Spitzenberger & Spies linear power amplifiers connecting the under-test GFL IBR work as a three-phase grid whose adjustable impedance makes SCCR = 10; Fig. 13 illustrates the test rig deployed. Figs. 14–16 depict the experimental results obtained for *Scenario I*, *Scenario II*, and

Scenario III of the GFL IBR using an LCL filter shown in Fig. 2. The experimental outcomes validate the effectiveness of the proposed control scheme based on the available resources.

G. Discussion on Simulations and Experimental Results

As evident from the results presented in this section, the GFL IBR equipped with the proposed control scheme demonstrates a remarkable ability to mitigate the deleterious effects of FDI cyber-attacks. When such attacks occur, both the three-phase and dq-frame current signals rapidly return to their reference values in a very short timeframe, specifically less than 0.05 seconds. The three-phase current signal effectively maintains its sinusoidal shape with a THD of less than %0.2—which is within the permissible range outlined by IEEE Std 1547.P10-2018 [13]. The error deviations of the active and reactive power from their setpoints are approximately %0.1, a negligible error compared with the scale of output powers. While the conventional PI controller performs perfectly well in terms of reference tracking under normal circumstances, it fails to swiftly return the signals of interest to their nominal values in the presence of FDI attacks. In particular, the peak-to-peak value of the three-phase current signal surges up to 6 pu, impacting the proper functioning of IBRs.

V. Conclusion

This paper has proposed a resilient control framework for in situ primary control of the grid-following inverter-based resources to mitigate the destructive effects of false data injection cyber-attacks. The adversary may attempt to insert malicious data into the control channels of pulse width modulators. The proposed control scheme integrated and augmented with auxiliary dynamics has ensured stability and output tracking regardless of the occurrence of a false data injection cyber-attack. Additionally, the paper has introduced a thorough stability analysis based on Lyapunov principles and discussed the factors to consider in designing the control matrices. The performance and efficacy of the suggested control scheme have been further validated by comparative MATLAB/Simulink simulations and tested by experimental results. The future direction of this study aims to extend the proposed control scheme to address false data injection attacks on sensors and even setpoint values in grid-following inverter-based resources under weak-grid conditions.

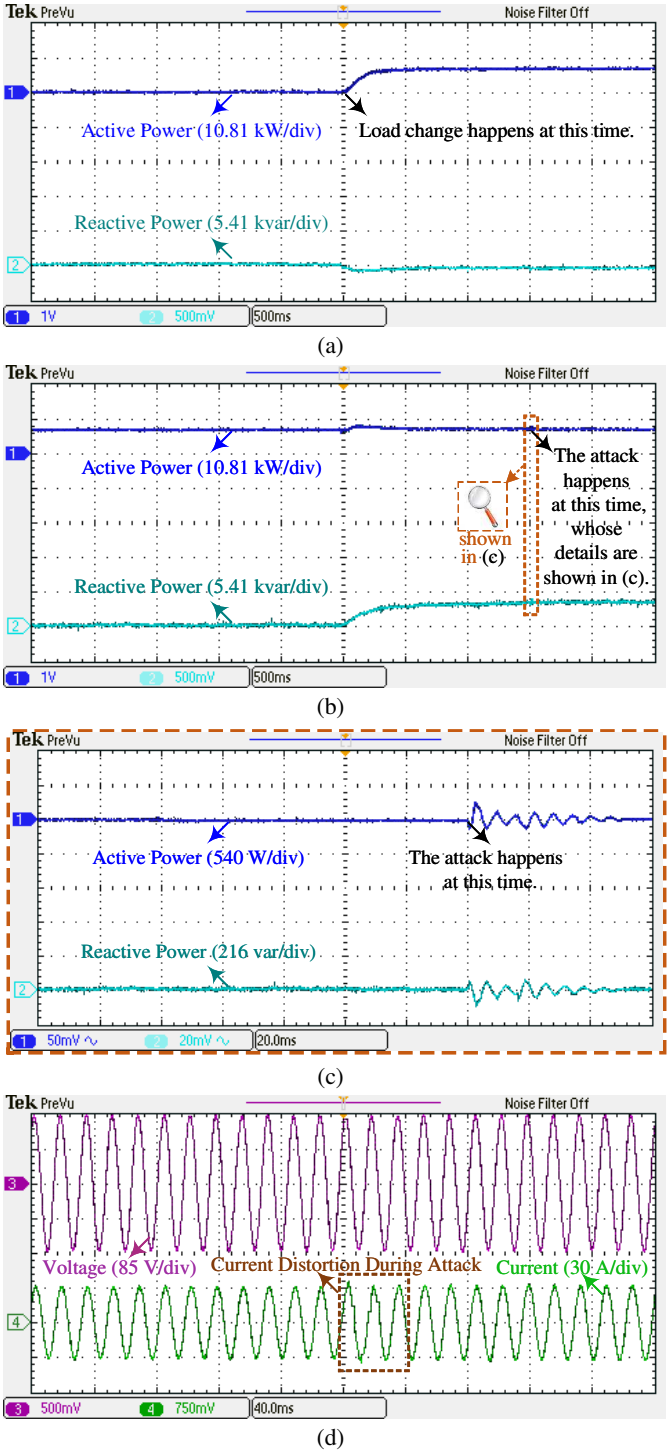

Fig. 14. Experimental results of *Scenario I*: (a) the active power increase with 10.81 kW/div [vertical axis for active power (P)] and 500 ms/div (horizontal axis), (b) the reactive power increase with 5.41 kvar/div [vertical axis for reactive power (Q)] and 500 ms/div (horizontal axis), (c) transients shown in Fig. 14 (b) by capturing its ac component with 540 W/div (vertical axis for P), 216 var/div (vertical axis for Q), and 20 ms/div (horizontal axis) when the attack (d) voltage 85 V/div (vertical axis), 30 A/div (vertical axis), and 40 ms/div (horizontal axis).

References

[1] Q. Liu, T. Caldognetto, and S. Buso, "Review and comparison of grid-tied inverter controllers in microgrids," *IEEE Transactions on Power Electronics*, vol. 35, no. 7, pp. 7624–7639, 2019.

[2] S. K. Mazumder, A. Kulkarni, S. Sahoo, F. Blaabjerg, H. A. Mantooth, J. C. Balda, Y. Zhao, J. A. Ramos-Ruiz, P. N. Enjeti, P. Kumar *et al.*, "A review of current research trends in power-electronic innovations in cyber–physical systems," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5146–5163, 2021.

[3] L. Shi, Q. Dai, and Y. Ni, "Cyber–physical interactions in power systems: A review of models, methods, and applications," *Electric Power Systems Research*, vol. 163, pp. 396–412, 2018.

[4] M. K. Kagita, G. R. Bojja, and M. Kaosar, "A framework for intelligent iot firmware compliance testing," *Internet of Things and Cyber-Physical Systems*, vol. 1, pp. 1–7, 2021.

[5] M. Davari, M. P. Aghababa, F. Blaabjerg, and M. Saif, "An innovative, adaptive faulty signal rectifier along with a switching controller for reli-

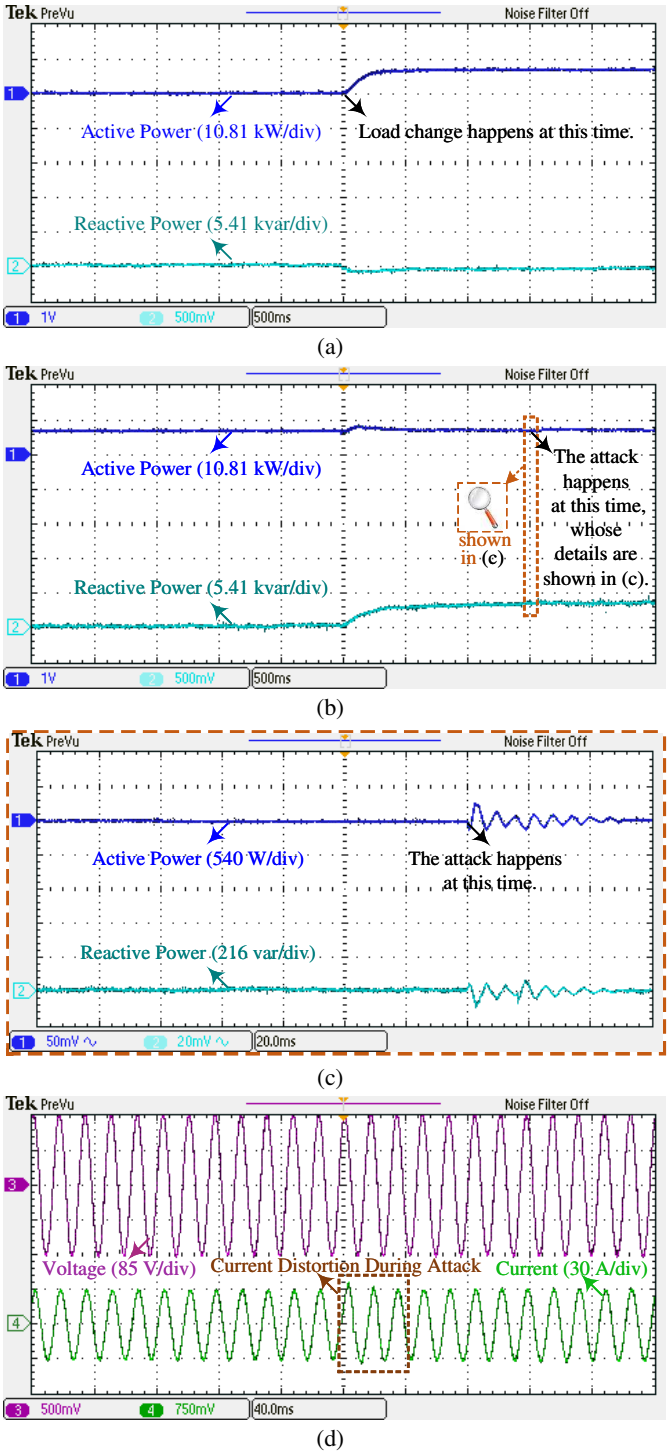

Fig. 15. Experimental results of *Scenario II*: (a) the active power increase with 10.81 kW/div [vertical axis for active power (P)] and 500 ms/div (horizontal axis), (b) the reactive power increase with 5.41 kvar/div [vertical axis for reactive power (Q)] and 500 ms/div (horizontal axis), (c) transients shown in Fig. 14 (b) by capturing its ac component with 540 W/div (vertical axis for P), 216 var/div (vertical axis for Q), and 20 ms/div (horizontal axis) when the attack (d) voltage 85 V/div (vertical axis), 30 A/div (vertical axis), and 40 ms/div (horizontal axis)

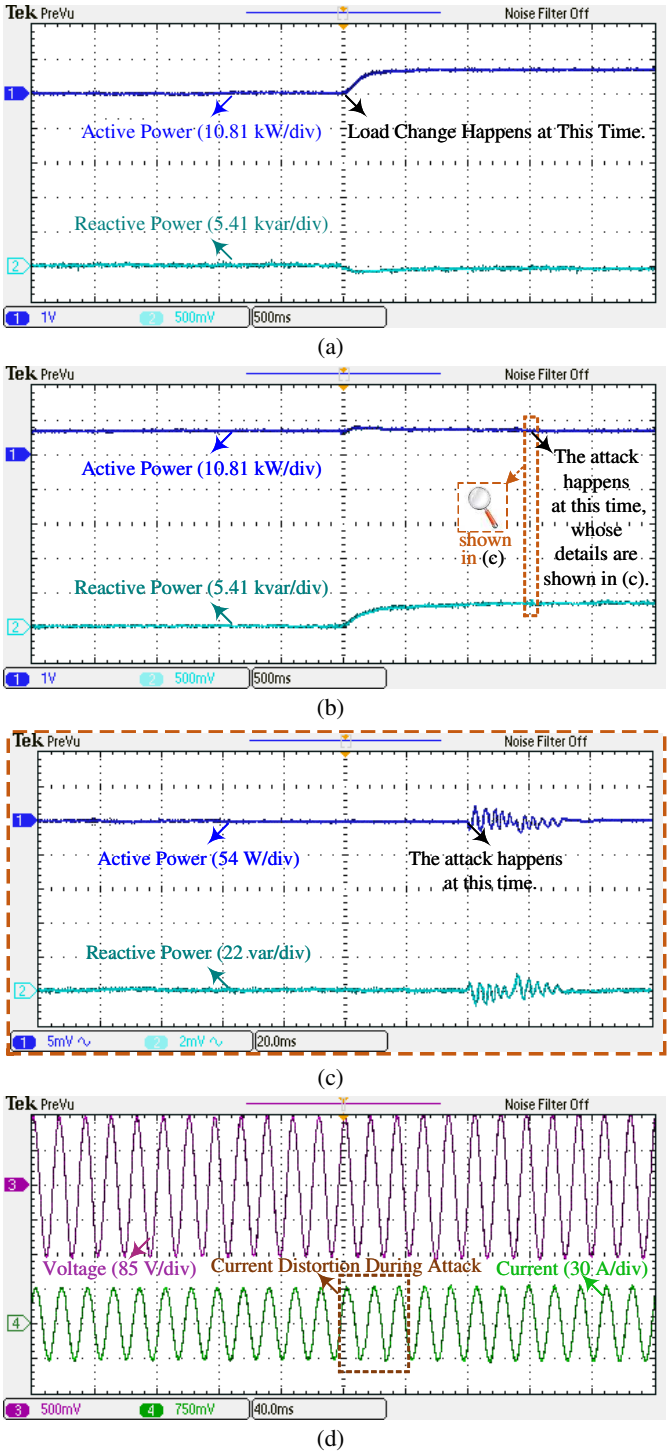

Fig. 16. Experimental results of *Scenario III*: (a) the active power increase with 10.81 kW/div [vertical axis for active power (P)] and 500 ms/div (horizontal axis), (b) the reactive power increase with 5.41 kvar/div [vertical axis for reactive power (Q)] and 500 ms/div (horizontal axis), (c) transients shown in Fig. 16 (b) by capturing its ac component with 54 W/div (vertical axis for P), 22 var/div (vertical axis for Q), and 20 ms/div (horizontal axis) when the attack (d) voltage 85 V/div (vertical axis), 30 A/div (vertical axis), and 40 ms/div (horizontal axis).

able primary control of GC-VSIs in CPS-based modernized microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 7, pp. 8370–8387, 2021.

[6] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid,"

Electricity Information Sharing and Analysis Center (E-ISAC), vol. 388, pp. 1–29, 2016.
[7] H. Goyel and K. S. Swarup, "Data integrity attack detection using ensemble based learning for cyber physical power systems," *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1198–1209, 2022.
[8] Y. Li and Y. Wang, "Developing graphical detection techniques for maintaining state estimation integrity against false data injection attack in integrated electric cyber-physical system," *Journal of Systems Architecture*, vol. 105, p. 101705, 2020.
[9] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2871–2881, 2018.
[10] R. Tan, H. H. Nguyen, E. Y. Foo, D. K. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1609–1624, 2017.
[11] H. Ibrahim, J. Kim, P. Enjeti, P. Kumar, and L. Xie, "Detection of cyber attacks in grid-tied PV systems using dynamic watermarking," in *2022 IEEE Green Technologies Conference (GreenTech)*. IEEE, 2022, pp. 57–61.
[12] J. Ramos-Ruiz, J. Kim, W.-H. Ko, T. Huang, P. Enjeti, P. Kumar, and L. Xie, "An active detection scheme for cyber attacks on grid-tied PV systems," in *2020 IEEE CyberPELS (CyberPELS)*. IEEE, 2020, pp. 1–6.
[13] IEEE Standards Coordinating Committee 21, "1547-2018 - IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," IEEE Std 1547, Tech. Rep., 2018.
[14] M. Jamali, M. S. Sadabadi, M. Davari, S. Sahoo, and F. Blaabjerg, "Resilient cooperative secondary control of islanded ac microgrids utilizing inverter-based resources against state-dependent false data injection attacks," *IEEE Transactions on Industrial Electronics*, vol. 71, no. 5, pp. 4719–4730, 2023.
[15] M. Jamali, H. R. Baghaee, M. S. Sadabadi, G. B. Gharehpetian, and A. Anvari-Moghaddam, "Distributed cooperative event-triggered control of cyber-physical AC microgrids subject to denial-of-service attacks," *IEEE Transactions on Smart Grid*, vol. 14, no. 6, pp. 4467–4478, 2023.
[16] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annual Reviews In Control*, vol. 47, pp. 394–411, 2019.
[17] M. Jafari, M. A. Rahman, and S. Paudyal, "False data injection attack against power system small-signal stability," in *2021 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2021, pp. 1–5.
[18] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151 019–151 064, 2020.
[19] M. G. Angle, S. Madnick, J. L. Kirtley, and S. Khan, "Identifying and anticipating cyberattacks that could cause physical damage to industrial control systems," *IEEE Power and Energy Technology Systems Journal*, vol. 6, no. 4, pp. 172–182, 2019.
[20] M. Jamali, M. S. Sadabadi, and A. Oshnoei, "Cyber-resilient adaptive control of grid-following inverter-based resources against measurement manipulation," in *25th IEEE International Conference on Industrial Technology*, 2024.
[21] Y. Li and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Transactions on Power Electronics*, vol. 38, no. 2, pp. 2364–2383, 2022.
[22] SMA inverter firmware update. Accessed: November 10, 2023. [Online]. Available: https://manuals.sma.de/SBx1SPUS40/en-US/1165323019.html
[23] Remote firmware upgrades via iSolarCloud. Accessed: August 8, 2023. [Online]. Available: https://manuals.sma.de/SBSxx-US-10/en-US/index.html
[24] R. Akkaoui, A. Stefanov, P. Palensky, and D. H. Epema, "Resilient, auditable and secure IoT-enabled smart inverter firmware amendments with blockchain," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 8945–8960, 2024.
[25] B. Ahn, T. Kim, S. Ahmad, S. K. Mazumder, J. Johnson, H. A. Mantooth, and C. Farnell, "An overview of cyber-resilient smart inverters based on practical attack models," *IEEE Transactions on Power Electronics*, 2023.
[26] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters—challenges and vulnerabilities," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5326–5340, 2019.
[27] M. Amin, F. F. El-Sousy, G. A. A. Aziz, K. Gaber, and O. A. Mohammed, "CPS attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: A review," *IEEE Access*, vol. 9, pp. 38 571–38 601, 2021.
[28] M. Gursoy and B. Mirafzal, "On self-security of grid-interactive smart inverters," in *2021 IEEE Kansas Power and Energy Conference (KPEC)*. IEEE, 2021, pp. 1–6.
[29] ——, "Self-security for grid-interactive smart inverters using steady-state reference model," in *2021 IEEE 22nd Workshop on Control and Modelling of Power Electronics (COMPEL)*. IEEE, 2021, pp. 1–5.
[30] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, "Secure internet of things (IoT)-based smart-world critical infrastructures: Survey, case study and research opportunities," *IEEE Access*, vol. 7, pp. 79 523–79 544, 2019.
[31] D. E. Olivares, A. Mehrizi-Sani, A. H. Etemadi, C. A. Cañizares, R. Iravani, M. Kazerani, A. H. Hajimiragha, O. Gomis-Bellmunt, M. Saeedifard, R. Palma-Behnke, G. A. Jiménez-Estévez, and N. D. Hatziargyriou, "Trends in microgrid control," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1905–1919, 2014.
[32] J. D. Mireles, E. Ficke, J.-H. Cho, P. Hurley, and S. Xu, "Metrics towards measuring cyber agility," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3217–3232, 2019.
[33] R. A. Horn and C. R. Johnson, *Matrix analysis*, 2nd ed. New York, NY, USA: Cambridge University Press, 2012.
[34] H. K. Khalil, *Nonlinear systems*. 3rd ed. London, U.K.: Prentice-Hall, 2002.
[35] S. Puntanen, G. P. Styan, and J. Isotalo, *Matrix tricks for linear statistical models: our personal top twenty*. Springer, 2011.
[36] M. Wu, B. Yin, A. Vosoughi, C. Studer, J. R. Cavallaro, and C. Dick, "Approximate matrix inversion for high-throughput data detection in the large-scale MIMO uplink," in *2013 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2013, pp. 2155–2158.
[37] R. Khezri, S. Shokoohi, S. Golshannavaz, and H. Bevrani, "Intelligent over-current protection scheme in inverter-based microgrids," in *2015 Smart Grid Conference (SGC)*. IEEE, 2015, pp. 53–59.
[38] J. Lofberg, "Yalmip: A toolbox for modeling and optimization in matlab," in *2004 IEEE International Conference on Robotics and Automation (IEEE Cat. No. 04CH37508)*. IEEE, 2004, pp. 284–289.
[39] A. Yazdani and R. Iravani, *Voltage-sourced converters in power systems: modeling, control, and applications*. John Wiley & Sons, 2010.
[40] S. Silwal, M. Karimi-Ghartemani, H. Karimi, M. Davari, and S. M. H. Zadeh, "A multivariable controller in synchronous frame integrating phase-locked loop to enhance performance of three-phase grid-connected inverters in weak grids," *IEEE Transactions on Power Electronics*, vol. 37, no. 9, pp. 10 348–10 359, 2022.
[41] M. Davari, M. P. Aghababa, F. Blaabjerg, and M. Saif, "A modular adaptive robust nonlinear control for resilient integration of vsis into emerging modernized microgrids," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 3, pp. 2907–2925, 2021.
[42] S. Silwal, S. Taghizadeh, M. Karimi-Ghartemani, M. J. Hossain, and M. Davari, "An enhanced control system for single-phase inverters interfaced with weak and distorted grids," *IEEE Transactions on Power Electronics*, vol. 34, no. 12, pp. 12 538–12 551, 2019.
[43] M. Davari and Y. A.-R. I. Mohamed, "Robust vector control of a very weak-grid-connected voltage-source converter considering the phase-locked loop dynamics," *IEEE Transactions on Power Electronics*, vol. 32, no. 2, pp. 977–994, 2017.

Mahmood Jamali received the B.Sc. degree in Electrical-Control Engineering from the Ferdowsi University of Mashhad, Mashhad, Iran, in 2017, and the M.Sc. degree in Control Engineering from the Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in 2020, respectively. He is pursuing a Ph.D. in Automatic Control and System Engineering at the University of Sheffield, United Kingdom. His research interests focus on control systems and their applications in modern power grids and power electronic converters.

Mahdieh S. Sadabadi (Senior Member, IEEE) is an Assistant Professor at the Department of Electrical and Electronic Engineering at The University of Manchester, Manchester, U.K. Previously, she held academic positions at Queen Mary University of London and the University of Sheffield. She was a Postdoctoral Research Associate at the Department of Engineering, at the University of Cambridge, and a Postdoctoral Fellow in the Division of Automatic Control, Linkoping University in Sweden. She received her Ph.D. in Control Systems from the Swiss Federal Institute of Technology in Lausanne (EPFL), Switzerland in February 2016. Her research focuses on fundamental theoretical and applied research on robust, resilient, secure, and scalable control strategies for cyber-physical systems under uncertainty. Her research is inspired by the control and resilience challenges involved in integrating and interconnection of power electronics converters into future power networks.

Subham Sahoo (Senior Member, IEEE) received the Ph.D. degree in Electrical Engineering from Indian Institute of Technology, Delhi, India in 2018. He is currently an Assistant Professor in the Department of Energy, Aalborg University (AAU), Denmark, where he is also the vice-leader of the research group on Reliability of Power Electronic Converters (ReliaPEC) in AAU Energy. He has previously been employed as a postdoc in NUS Singapore and has had visiting appointments with MIT, Cardiff University and University of Edinburgh over the years.

His work on cybersecurity in power electronics and system resiliency has received recognitions from Indian National Academy of Engineering (INAE), EU-US National Academy of Engineering (NAE) Frontier of Engineering (FOE) and has also been featured in the media, Videnskab.dk and ScienceNordic. He was a distinguished reviewer for IEEE Transactions on Smart Grid in 2020. He is the nation-wide mentor in Denmark for neuromorphic computing in Danish Data Science Academy (DDSA) and an affiliate of the Lundbeck Foundation Investigator Network (LFIN).

He is the vice-chair of IEEE Power Electronics Society (PELS) Technical Committee (TC) 10 on Design Methodologies. His research interests are sustainable, probabilistic AI and their applications in power electronic grids.

Masoud Davari (Senior Member, IEEE) was born in Isfahan, Iran, in 1985. He received the B.Sc. degree (summa cum laude) in electrical engineering (power) from the Isfahan University of Technology, Isfahan, in 2007, the M.Sc. degree (summa cum laude) in electrical engineering (power) from the Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in 2010, and the Ph.D. degree in electrical engineering [power electronics in energy systems (summa cum laude)] from the University of Alberta, Edmonton, AB, Canada, in 2016.

He was with Iran's Grid Secure Operation Research Center and Iran's Electric Power Research Institute (EPRI), Tehran, Iran, from January 2010 to December 2011. From April 2015 to June 2017, he was a Senior R & D Specialist and Senior Consultant with Quanta-Technology Company, Markham, ON, Canada, in the field of the dynamic interaction of renewables with smart ac/dc grids and control, protection, and automation of microgrids. In July 2017, he joined as a tenure-track Assistant Professor with the Allen E. Paulson College of Engineering and Computing, Department of Electrical and Computer Engineering, Georgia Southern University (GSU), Statesboro, GA, USA—where he was recommended for being granted "*early*" promotion to Associate Professor and award of "*early*" tenure on December 3, 2021, and officially approved for both on February 16, 2022. He is the Founder and the Director of the Laboratory for Advanced Power and Energy Systems (LAPES) in the state-of-the-art Center for Engineering and Research established in 2021 with GSU—LAPES can be toured online via the https://www.youtube.com/watch?v=mhVHp7uMNKo YouTube link. He has developed and implemented several experimental test rigs for research universities and the power and energy industry. He has also authored several papers published in IEEE Transactions and journals. His research interests include the dynamics, controls, and protections of different power electronic converters utilized in the hybrid ac/dc smart grids and modern power and energy systems testing based on different hardware-in-the-loop (HIL) simulations.

Dr. Davari has been an active member of and a chapter lead (for Chapter 3) in the IEEE Working Group P2004—a newly established IEEE working group entitled "*Hardware-in-the-Loop (HIL) Simulation Based Testing of Electric Power Apparatus and Controls*" for the IEEE Standards Association since June 2017. He was an active member of and a chapter lead in the IEEE Power & Energy Society Task Force on "*Innovative Teaching Methods for Modern Power and Energy Systems*" from 2020 to 2024. He was the Chair of the Literature Review Subgroup of DC@Home Standards for the IEEE Standards Association from April 2014 to October 2015. He is an invited reviewer of several of the IEEE TRANSACTIONS/JOURNALS, IET journals, *Energies* journal, and various IEEE conferences, the invited speaker at different universities and in diverse societies, and the Best Reviewer of the IEEE TRANSACTIONS ON POWER SYSTEMS in 2018 and 2020. He was an invited member of the Golden Key International Honour Society. He was the recipient of the 2019–2020 Allen E. Paulson College of Engineering and Computing Faculty Award for Outstanding Scholarly Activity in the Allen E. Paulson College of Engineering and Computing at GSU, the Discovery & Innovation Award from the 2020–2021 University Awards of Excellence at GSU, and one of the awardees of the 2021–2022 Impact Area Accelerator Grants (partially funded) at GSU. His biography has been included in *Marquis Who's Who* biographies since 2023. The Awards Committee of the American Society for Engineering Education (ASEE) designated him as the "*finalist*" for the 2024 Curtis W. McGraw Research Award in February 2024.

Frede Blaabjerg (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Aalborg University, Aalborg, Denmark, in 1995. From 1987 to 1988, he was with ABBScandia, Randers, Denmark. He became an Assistant Professor, an Associate Professor, and a Full Professor of power electronics and drives at Aalborg University in 1992, 1996, and 1998, respectively. In 2017, he became a Villum Investigator. Additionally, he is Honoris Causa with the University Politehnica Timisoara (UPT), Timisoara, Romania, and Tallinn Technical University, Tallinn, Estonia.

Dr. Blaabjerg has authored or co-authored four monographs and published more than 600 journal articles in various fields of power electronics and its applications; he was an editor of ten books on power electronics and its applications. His current research interests include power electronics and its applications, such as in wind turbines, PV systems, reliability, harmonics, and adjustable speed drives. He was a recipient of the 33 IEEE Prize Paper Awards, the IEEE PELS Distinguished Service Award in 2009, the EPE-PEMC Council Award in 2010, the IEEE William E. Newell Power Electronics Award in 2014, the Villum Kann Rasmussen Research Award in 2014, the Global Energy Prize in 2019, and the 2020 IEEE Edison Medal. From 2006 to 2012, he was the Editor-in-Chief for the IEEE TRANSACTIONS ON POWER ELECTRONICS. From 2005 to 2007, he was a Distinguished Lecturer of the IEEE Power Electronics Society and the IEEE Industry Applications Society from 2010 to 2011 and from 2017 to 2018. From 2019 to 2020, he was the President of the IEEE Power Electronics Society. He was the Vice President of the Danish Academy of Technical Sciences, Lyngby, Denmark. From 2014 to 2020, he was nominated by Thomson Reuters, Toronto, Canada, to be among the 250 most cited researchers in engineering in the world.