On Self-Security of Grid-Interactive Smart Inverters

Mehmetcan Gursoy, *Student Member, IEEE,* and Behrooz Mirafzal, *Senior Member, IEEE*

***Abstract*— The capability to exchange information with utility operators, aggregators, and nearby smart devices can make a grid-interactive inverter an intelligent cyber-physical device. However, the capability of exchanging information can also put the inverters at the risk of insecure operation. In this paper, possible software manipulations into the inverters are studied to understand their vulnerability to cyberattacks. Moreover, the state-of-the-art system-level and device-level cyber-defense measures are discussed, and advantages and drawbacks of each technique are provided. Studies show that a reference model can be implemented in device-level security to effectively examine incoming setpoints for detecting and preventing malicious or harmful actions. This paper particularly underlines the significance of device-level self-security and its advantages for grid-interactive inverters. Finally, recommendations for future studies are provided.**

***Index Terms*— Smart inverters, cyber-physical systems, self-security, self-learning, inverter operating region, malicious setpoints, machine learning, cyber-security, false-data-injection.**

I. INTRODUCTION

The conventional power grid is rapidly evolving to a cyber-physical structure due to the global tendency to renewable energy resources and the increase of distributed generation units. Smart inverters provide controllable interfaces that bridge the cyber network with physical devices. These devices can also provide ancillary services to regulate the voltage and harmonic compensations. Recent investigations demonstrate that inverters can operate in grid-forming mode to form networked microgrids with black-start capabilities [1]-[4]. The grid-interactive smart inverters are the backbone of the modern power grid, allowing high integration of renewable energy sources with remote and dynamic control features at a lower cost. For instance, California's total solar power generation is nearly 13%, except for some areas offering about 25% [5]. California has a goal-setting of utilizing 50% renewable energy generation by 2030 [6].

Communication feature enables information exchange between physical devices across the power grid through wired or wireless wide-area-network (WAN) or local-area-network (LAN). Thus, system monitoring devices, advanced metering infrastructures (AMIs), and Internet-of-Things (IoT) enabled devices can be employed for data sharing to allow autonomous interactions for the inverters. However, providing more access surfaces on the internet cause smart inverters to be highly vulnerable to cyber-attacks. If these attacks are deliberately made from secured sources with authorized access, such as a utility grid operator, the manipulated data can bypass the security protocols [7]. This can result in data modifications such as supervisory commands, measured system data, or power setpoints that can yield asymmetrical and abnormal operation, excessive power injection, etc. [4]. Under such circumstances, a system recovery might not even be possible. This can cause equipment destruction and large-scale blackouts that can lead to high economic considerations [5]-[8]. Power outages in 2015 and 2016 in Ukraine are examples of malicious attacks that happened due to hacking the grid supervisory control and data acquisition (SCADA) [8].

To minimize the concerns about malicious attacks and achieve safer operation under these attacks, the utmost attention must be paid to cyber-security. Therefore, anomaly detection and attack prevention play vital roles in avoiding potential malicious attacks [7]. Former investigations promote improved communication and data-transfer security, falling into the basic network security category, to prevent cyber-attacks [8], [9]. Some researchers applied data-driven approaches such as machine learning-based heuristic algorithms [7], [8], [10]-[12], where the results are compared with the developed model. Nonetheless, authors in [7], [13], and [14] have focused on knowledge-based techniques where measured values with any time-dependent threshold are compared with the known constant values to detect cyberattacks. All developed techniques aim to improve the level of security against cyber threats. Furthermore, a device-level model-based self-security functionality for smart inverters is proposed and experimentally tested in [7] to examine the validity of the incoming setpoints. On the other hand, the model-based security is also addressed in [15] using a general mathematical model as the trajectories are bounded by a radius, and abnormal operation is detected when the trajectories are out of the bounded area.

This article provides a better understanding of power electronics-based cyber-physical systems, particularly smart inverters. In this paper, cyberattack vulnerabilities and possible data modification attack scenarios are discussed. Consequently, ongoing attack prevention techniques are reviewed to keep up with the latest progress along with the state-of-the-art system- and device-level defense methodologies. Finally, some gaps for the discussed techniques are provided to call attention to future research opportunities.

In addition to the introduction, the paper contains four more sections. Section II presents the cyber-physical system where possible cyber threats can be performed. Also, the vulnerable points of cyber-physical systems are identified in this section. Section III elaborates on possible cyber-attack scenarios for the inverters and their impacts on the overall system. Section IV reviews the literature that proposed solutions to detect and prevent malicious activities. Finally, in section V, the conclusion and recommendation for future study are given.

This material is based upon work supported by the Department of Energy, Office of Energy Efficiency and Renewable Energy (EERE), Solar Energy Technologies Office, under Award Number DE-EE0008767.

II. Cyber-Physical System and Types of Possible Attacks

The next-generation smart devices such as smart inverters, phasor measurement units (PMUs), meters, etc., can link cyber networks with physical devices, also known as cyber-physical devices. These smart devices can communicate, share data, and executive commands in real-time to improve the overall system's performance, efficiency, and reliability. For instance, Fig. 1 shows that a smart inverter can receive commands from the utility supervisory controller or a third-party aggregator through a communication link to disconnect from the grid or update PQ setpoints to manage the power demand. Similarly, smart inverters connected to a grid of microgrids, also known as networked microgrids, can share their measurements, operating points, or system status data using the centralized controller or their local controllers. Making grid-interactive inverters intelligent allows inverters to operate beyond grid-feeding mode, such as grid-supporting (ancillary services) and grid-forming modes of operation [1], [16], [17]. Furthermore, inverters located in a neighborhood can form a clustered data communication network to reduce the impact of cyberattacks.

The main challenge in cyber-physical device operation is to maintain security as hackers intentionally focus on jeopardizing the device operation. Notably, the inverter-based low inertia power systems are more sensitive to instant changes that can potentially lead to voltage sags or swells and cascaded inverter trips [18]. Insecure network and communication protocols, outdated authentication, and weak points in the software are the main reasons that the attackers can breach the system through the cyber network, as shown in Fig. 1, and perform data modification. To develop methodologies and prevent cyberattacks, common types of attacks should be known, see Fig. 2. Attack types and their objectives targeting intelligent devices connected to the cyber network are listed based on the research conducted in [6], [8], and [19]. The outcomes of successful attacks highly depend on the level of information a hacker can obtain for each device. In the next section, possible cyberattack scenarios and their outcomes will be presented.

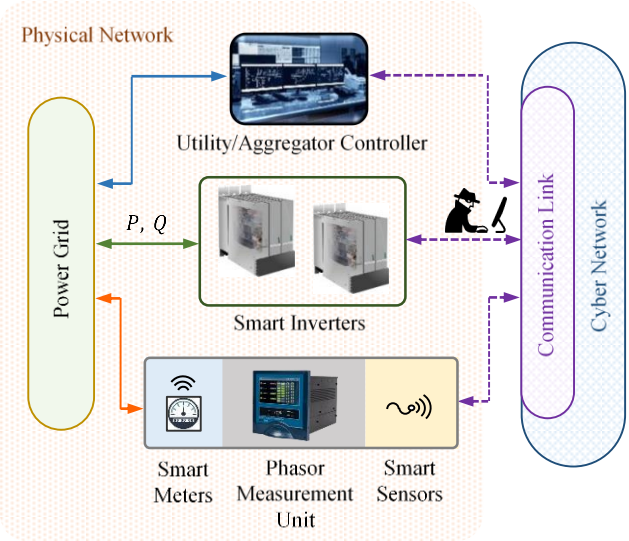

Fig. 1. Smart inverters connected to the power grid and cyber attacker targeting the communication link in a cyber-physical system.

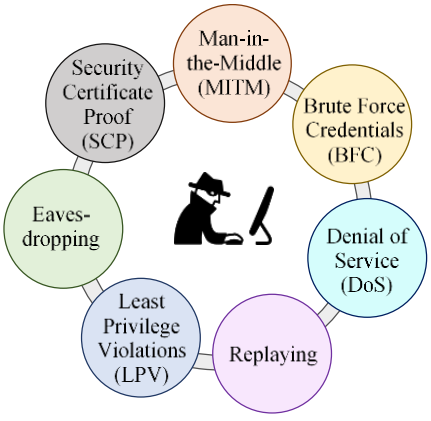

Fig. 2. Cyberattack vulnerabilities of cyber-physical inverters.

III. Possible Malicious Data Injection Scenarios and Their Impacts

The most well-known attack scenario is called false data injection (FDI). This scenario covers all attack types provided in Table I, except eavesdropping. Since the power control loops in inverters are not typically editable due to the read-only memory operation, only the external data such as reference setpoints, data communication, tunable parameters, user interface software, and local feedback signals can be accessible in real-time [15]. This scenario is demonstrated in Fig. 3. Possible scenarios are given in the following subsections.

A. Sensor Data Modification

Typically, inverters are equipped with their own sensors and measurement units. Therefore, manipulating the inverter's sensor data requires physical access to the built-in sensors, which would less likely be the case. For a grid-interactive system, the state variables can be the system currents and voltages. If the inverters measure line currents, voltages, and frequency using external measurement units or sensors as depicted in Fig. 3, then SCP, MITM, LVP, or replaying intrusion actions can be accomplished by the attacker to modify the data sent to the inverters. The system dynamics can be influenced by altering the measured information, and this could endanger the inverter's operation. The system dynamics can also significantly change if the incoming data is replayed, blocked, or jammed.

TABLE I
Objectives of Cyberattack Types Against Smart-Inverters

Types of Attacks	Description
Security Certificate Proof (SCP)	Unauthorized access to key certificates.
Man-in-the-Middle (MITM)	Unauthorized access between two parties.
Brute Force Credentials (BFC)	Predicting user log-in information.
Denial of Service (DoS)	Jamming the network traffic.
Least Privilege Violations (LPV)	Accessing unauthorized functionalities.
Replaying	Repeating incoming data.
Eavesdropping	Obtaining information about the system.

B. Desired Operating Point Modification

The inputs of an inverter, such as the grid frequency, grid voltages, active and reactive power setpoints, and DC source voltage, vary depending on the local controller's processed control technique. Modification to the incoming data of an inverter is demonstrated in Fig. 3 as the attacker targets the incoming information. Like the sensor data modification, if the desired setpoints are manipulated, the inverter operation and system dynamics can be jeopardized. This can result in undesired power flow and fluctuations in grid voltages.

On the other hand, centralized control techniques feature data transfer between master and slave units to share phase and frequency information in a grid-forming mode of operation. This allows synchronization between the grid-forming inverters [20]-[22]. Receiving a manipulated data from the other inverter unit can put the system out of synchronization that can trip the inverters or intentionally activates the protective relays and provide insufficient power for the loads.

C. Malicious Commands Sent to Nearby Protection Devices

Cyberattacks can be performed bi-directional, and outgoing signals can be manipulated. For instance, the command signals from inverters and relays to static switches can be manipulated, see Fig. 3. In the event that the command signal is altered to prevent the relays from tripping, high current flow can happen from the grid to the inverters or vice versa, which can cause permanent damage to the inverters, cables, and loads.

Notice, risk arises when islanding is required, i.e., for maintenance operation or installing new equipment. To protect the workers during their operation, the operators must make sure that the smart inverters are disconnected from the grid or microgrid, and there are no other power sources that remain connected. In case of a successful malicious attack, the command sent to the protective relays or switches can be reset by manipulating the anti-islanding codes. The anti-islanding manipulation can put people at the risk of electric shocks and catastrophic failures while installing new equipment.

D. Forecasting Data Modification

In solar power applications, smart inverters can receive PV forecasting information from weather services every specified period using the cyber network. Based on the maximum available power at a certain time, a smart inverter can adjust its output power. An inverter can send a command to a utility or aggregator controller to increase the power generated from generators some short period before the forecasted event happens. This period allows the generator output to reach the required power level because the inertia of the generators does not allow instant changes, while the inverter gradually reduces its output power. In case an inverter receives malicious PV forecasting data, PV power can be curtailed, and power generated from the conventional sources will be increased. The curtailed power will be wasted if there are no energy storage units in the system. Moreover, actively increasing and decreasing the inverter and generator powers can cause stress on the equipment.

In the following section, investigations and methodologies developed to detect, mitigate, and/or prevent cyberattacks are discussed.

IV. Harmful Activity Detection and Defense

Cyberattack detection/prevention is a trending research area in recent years. Even though numerous research is conducted in this field, no investigation still ensures safe operation for cyber-physical devices. Techniques used to provide security can vary from advanced communication protocols to heavy computational processes, i.e., machine learning techniques. Some researchers use a model/knowledge-based approach when parameters are known or estimated to identify the attacks and maintain secure operation.

The basic security requirements for any cyber-physical system are user interface and network security. Attackers can successfully perform cyberattacks when their coding skills bypass the security protocols, authentication barriers, user interface firewall, etc. Existing measures focus on data transfer security. Current techniques are known as encryption and certificate-based authentication [6]. However, these measures are not sufficient to overcome the security challenges for smart inverters. According to [6], advanced cryptography techniques are needed to achieve safe data transfer during each transaction. To achieve an interoperable and plug-and-play platform for data exchange and device communication, cyber-security protocols and standards are established by organizations like IEEE and IEC [23]. For instance, communication protocols offered by IEC 61850 are listed in Table II [1], [24], [25]. Furthermore, a block-chain technique is presented in [26] to ensure integrity and authentication while maintaining cryptographic communication. Any intrusion will be alarmed to notify the user within the network package. Moreover, a message authentication code (MAC) is implemented in [8] to perform a validity check for the incoming data.

Besides cryptographic data transfer, long-term software support for security updates and operating system software is needed with restoring option [27]. While [6] suggests a trusted execution environment for safe data transfer between two parties, [27] recommends a "handshake" policy to provide an additional security layer before initiating the data transfer and after completing the transaction. Recently, National Renewable Energy Laboratory (NREL) introduced BlackRidge Transport Access Control (TAC) and Seclab Denelis Modbus Airlock that provide a multi-layer defense to detect cyber attacks [8].

Although these technologies can enhance communication security, there is always a chance that a skilled hacker can find a path to breach the security wall. On the other hand, most authentication and signature-based software protections fail if

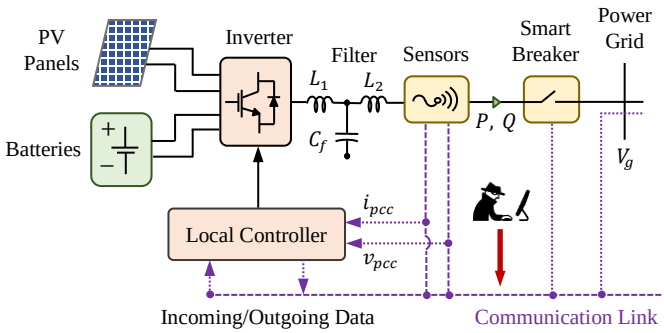

Fig. 3. A malicious attack scenario for a grid-interactive smart power electronics interface.

the malicious data is sent from an authorized source with authorized access, i.e., a third-party aggregator with obliterating intention interacts with grid-interactive inverters. When advanced network security and protocols fail, a hacker can attack the smart inverters through reference setpoints, tunable parameters, measured signals, and other external sensor data, as these are the only access points to perform a cyberattack. To accomplish safer operation and enhance the capabilities and smartness of the inverters, protection beyond the network security is essential. This can be achieved by developing methodologies using the system- and device-level information, as categorized in the following subsections.

A. System-Level Security

System-level defense uses system status and data sent from the nearby cyber-physical devices and controllers to examine whether there is malicious activity. Recent methodologies are heavily using data-driven approaches such as artificial intelligence (AI) and machine learning.

AI-based defense techniques are proposed in [28] and [29] to identify the FDI attacks. A nonlinear autoregressive exogenous model, a special type of recurrent neural network (RNN), is implemented in centralized DER controllers in DC microgrids in [28], whereas coordinated FDIs in DC microgrids are detected based on artificial neural networks (ANN) in [29]. On the other hand, a machine learning approach is proposed in [30] to detect FDI attacks. The authors developed a conditional deep belief network (CDBN) that features Conditional Gaussian-Bernoulli Restricted Boltzmann Machines (CGBRBM) to examine the real-time measurement data attack received from external sensors. A time-varying communication graph theory combined with a weighted mean subsequence reduced algorithm is applied in [31] to mitigate FDIs targeting inverter-based distributed energy resources (DERs) in microgrids. Lastly, a recursive systematic convolutional (RSC) method in [32] can be provided to detect the MITM attacks where the attack is oriented towards a supervisory controller linked to multiple distributed energy resources.

Artificial intelligence and machine learning algorithms require heavy computational burdens and days of offline training process. To develop data-driven methods, strong system knowledge is essential. Lack of system knowledge can result in weak training of the algorithm and can potentially lead to damages and high economic impacts. On the other hand, data-driven methodologies consume high power during the computational process.

Besides the data-driven approaches, there are some model/knowledge-based investigations in the literature. The model-based centralized and distributed detection methods are proposed in [13]. Another model-based partial primal-dual anomaly detection strategy is proposed in [33] for attacks targeting distributed secondary droop control in microgrids. The proposed technique only considers link and node attacks. Furthermore, the authors in [34] propose a distributed control framework for P-f control in AC microgrids using a virtual resilient layer with hidden networks. The event-driven approach introduced in [35] detects and mitigates stealth attacks occurring on the frequency control input in AC microgrids while ensuring resilient synchronization up to $N-1$ attacked units, where N represents the number of grid-forming inverters.

Watermarking is another approach to identify harmful attacks performed in the system. The idea of watermarking is to inject a signal into the system, detect the response at the gateway using a detector, and compare whether an error is observed in the measurement outcome [36]. This methodology typically provides authentication to the system and identifies spoofing, MITM, and FDI attacks. Dynamic authentication of IoT signals using a deep-learning-based long short-term memory structure is proposed in [37], and a game-theoretic framework that makes decisions by predicting sensitive IoT devices on the big scale is developed.

B. Device-Level Security

Even though many investigations have been reported about software and system-level securities, device-level detection is recommended in [6] using power electronics interfaces that shifts some inverter functionalities to energy buffer circuits to improve the voltage and frequency of ride-through capabilities, harmonics and unbalance distortions, or unintentional islanding. Energy storage devices will power these buffer circuits. However, the buffer inverters are not connected to a cyber network. Therefore, the term of smartness cannot be observed for the recommended buffer circuits.

A smart knowledge-based device-level self-security concept is first introduced by [7]. This model-based anomaly detection forms the backbone of device-level security. The authors emphasize that reference model-based defense methodologies could be developed to examine the integrity of incoming information at the device level. The concept of model-based self-defense is represented in Fig. 4. Herein, a smart inverter receives data, i.e., through a communication link. This data could include PQ setpoints from supervisory units such as utility and third-party controllers, measurement data from nearby devices such as other smart inverters, PMUs, and smart meters, and solar forecasting data from weather services. Before engaging the incoming data to the inverter's local controller, the security layer directs the data to the developed reference models. To enhance anomaly detection performance, multiple reference models can be equipped. In Fig. 4, some knowledge-based models are presented.

Depending on the designer's choice, reference models can be divided into two categories; (i) the fixed reference models, in which the model parameters are not updated in real-time, and (ii) adaptive reference models, in which model parameters such

TABLE II
IEC 61850 SECURITY PROTOCOLS

Protocol Name	Description
Manufacturing-Message-Specification (MMS)	Data exchange protocol between utility supervisory controller and cyber-physical devices.
Generic-Object-Oriented-Substation-Events (GOOSE)	Data exchange protocol between smart inverters.
Sample-Measured-Values (SMV)	Data exchange protocols from measurement units to smart inverters.

as grid parameters and PV forecasting data can be updated in real-time to represent the actual behavior or limits accurately. Furthermore, when enough knowledge is provided, a smart inverter can learn its dynamic performance, boundaries, and capabilities. Then, the inverter forms its reference models and automatically tune its parameter. The learning process becomes adaptive when adaptive reference models are utilized. This forms the concept of self-learning in self-security and allows inverters to make more accurate decisions under varying conditions comparing to the fixed reference models. Developed reference models examine the incoming information and send the expected output to the security unit that decides whether there is an anomaly or attack in the system. Notice, no matter where the data is received from, such as authorized or unauthorized sources, the incoming information is always checked using the knowledge-based models without bypassing the security layer. If an anomaly is detected, the received data is rejected, and the previous safe data remains in action. If the data is safe, it is engaged to the inverter's local controller.

In [7], anomalies or harmful activities are detected and prevented using three of the reference models shown in Fig.5 by; (i) checking the intersected area of the inverter's capability boundary, S_{max}, and (ii) instability boundary, using the theory from [38] and [39], and (iii) evaluating dynamic performance using a reduced-order dynamic model to represent the full-order dynamic behavior and to perform faster operations. The dynamic model is used to enhance the detection performance of the security algorithm. If the steady-state reference model detects anomalies, the incoming setpoints are examined using the dynamic reference model to verify whether the received setpoints might cause normal or abnormal operation. Parameter uncertainties can cause variations in the steady-state model, and the accepted setpoints can be detected as harmful setpoints or vice versa. However, the dynamic reference model can further verify whether these setpoints are harmful or not while parameters vary in real-time. The anomaly detection can be improved by adding PV forecasting data and updating S_{max}, accordingly.

Additional to the abovementioned models, requirements defined by IEEE Std. 1547-2018 such as high- and low- voltage ride-through, etc., can be implemented as another knowledge-based model to detect harmful activities. Smart inverters' responses under the defined scenarios can be monitored. Unexpected behavior, trips, or anti-islanding issues can be investigated. Moreover, utilizing the short-term inverter PQ setpoints memory as a reference model can be discussed as another point of view for attack detection. For instance, an inverter can record previously accepted setpoints and compare the incoming PQ setpoints with the recorded data. If a drastic change is detected, the incoming data can be rejected. This approach can further be extended by including past events. For instance, an inverter can learn which PQ setpoint ranges lead to abnormal operations or inverter trips from the experience and record these values as well as the rejected setpoints. Then, the algorithm can examine the new setpoints considering the past events.

Device-level security measures can be promising to identify stealth and authorized intentional attacks targeting the incoming data. When the reference models are properly formed, the system can protect itself and the grid from being damaged. On the other hand, the self-learning feature requires significantly less computational time and processing power than the machine-learning techniques. However, this concept must be used as an extra security layer. For instance, malicious external measurement data may cause an inaccurate calculation of the stability boundary, and harmful PQ setpoints may fall into the safe region. The security algorithm consequently might engage the setpoints to the inverter's local controller. The new setpoints can cause a sudden increase in active and/or reactive power due to the incoming malicious data and might result in voltage sags and swell at the point of common coupling. If secured network communication is established, and a proper system-level methodology is also equipped, sensor data attacks and anomalies can be detected.

V. Conclusion and Recommendations

In this paper, a brief cyber-security assessment for the grid-interactive smart inverters has been analyzed. At first, a cyber-physical system was described. Then, the cyber vulnerabilities for the inverters were introduced. Next, possible attack scenarios targeting the grid-supporting, grid-following, and grid-forming inverters as well as the attack limitation are provided. Furthermore, cutting-edge defense methodologies against cyberattacks that are available in the literature were reviewed to update some of the existing knowledge with recent investigations. Advanced methodologies were categorized in the form of system-level and device-level security. The existing communication protocols, network security, and system-level security measures do not ensure complete protection since authentication, cryptographic, and data-driven approaches can be bypassed by harmful incoming data intentionally sent by an

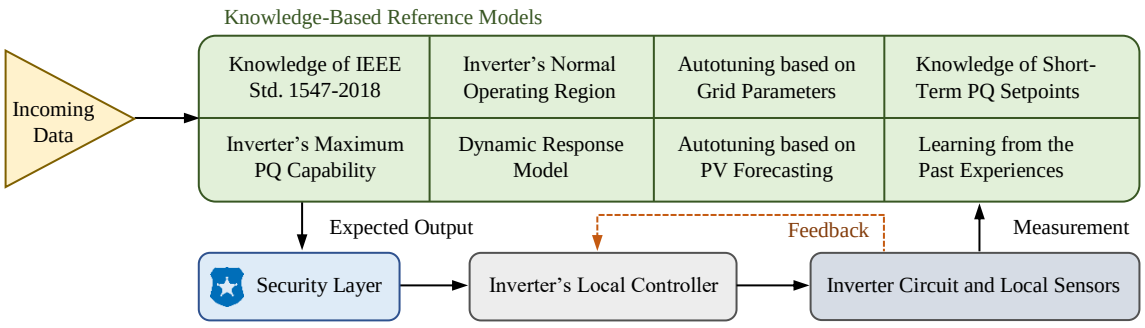

Fig. 4. The concept of model/knowledge-based self-security approach to detect cyberattacks. Combination of the reference model and the security layer forms device-level security.

authorized source using priority messages through authorized channels.

To enhance the security, ensure safe operation, protect the system devices being damaged, and maintain the integrity and normal operation, advanced, accurate, and fast attack detection and prevention techniques will always be in demand. Since each technique has advantages and disadvantages, and no methodology can ensure 100% cyber-physical security for a system, multi-stage/level protection techniques need to be developed. For safer inverter operation, model-based device-level self-security techniques need to be developed to provide additional protection and fill the gaps that the software- and system-level techniques cannot. Therefore, the necessity of device-level protection measures is emphasized since smart inverters and the utility equipment can be protected, and normal operation can still be observed under cyberattacks.

VI. References

[1] B. Mirafzal and A. Adib, "On grid-interactive smart inverters: features and advancements," *IEEE Access*, vol. 8, pp. 160526-160536, 2020.

[2] A. Adib and B. Mirafzal, "Virtual inductance for stable operation of grid-interactive voltage source inverters," *IEEE Trans. Ind. Electron.*, vol. 66, no. 8, pp. 6002-6011, Aug. 2019.

[3] A. Adib, J. Lamb and B. Mirafzal, "Ancillary services via VSIs in microgrids with maximum DC-bus voltage utilization," *IEEE Trans. Ind. Appl*., vol. 55, no. 1, pp. 648-658, Jan.-Feb. 2019.

[4] T. S. Ustun, J. Hashimoto and K. Otani, "Impact of smart inverters on feeder hosting capacity of distribution networks," *IEEE Access*, vol. 7, pp. 163526-163536, 2019.

[5] D. J. Sebastian and A. Hahn, "Exploring emerging cybersecurity risks from network-connected DER devices," *2017 North American Power Symposium (NAPS)*, Morgantown, WV, 2017, pp. 1-6.

[6] J. Qi, A. Hahn, X. Lu, J. Wang and C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Physical Syst.: Theory Appl*., vol. 1, no. 1, pp. 28-39, 12 2016.

[7] T. Hossen, F. Sadeque, M. Gursoy, and B. Mirafzal, "Self-secure inverters against malicious setpoints," *2020 IEEE Electric Power and Energy Conference (EPEC)*, Edmonton, AB, Canada, 2020, pp. 1-6.

[8] D. Saleem, A. Sundararajan, A. Sanghvi, J. Rivera, A. I. Sarwat and B. Kroposki, "A multidimensional holistic framework for the security of distributed energy and control systems," *IEEE Syst. J.*, vol. 14, no. 1, pp. 17-27, March 2020.

[9] S. K. Mazumder *et al*., "A Review of Current Research Trends in Power-Electronic Innovations in Cyber-Physical Systems," in *IEEE J. Emerg. Sel. Topics Power Electron*.

[10] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[11] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.

[12] K. Abdollah, W. Su, and T. Jin, "A machine learning based cyber attack detection model for wireless sensor networks in microgrids," *IEEE Trans. Ind. Informat.*, Jan. 2020.

[13] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, *vol*. 58, no. 11, pp. 2715–2729, Nov. 2013.

[14] Y. Shoukry and P. Tabuada, "Event-triggered state observers for sparse sensor noise/attacks," *IEEE Trans. Autom. Control*, vol. 61, no. 8, pp. 2079–2091, Aug. 2015.

[15] S. Sahoo, T. Dragičević and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters–challenges and vulnerabilities," *IEEE J. Emerg. Sel. Topics Power Electron.*

[16] A. Adib, F. Fateh and B. Mirafzal, "Smart inverter stability enhancement in weak grids using adaptive virtual-inductance," *IEEE Trans. Ind. Appl.*, vol. 57, no. 1, pp. 814-823, Jan.-Feb. 2021.

[17] R. H. Lasseter, Z. Chen and D. Pattabiraman, "Grid-forming inverters: A critical asset for the power grid," *IEEE J. Emerg. Sel. Topics Power Electron*, vol. 8, no. 2, pp. 925-935, June 2020.

[18] O. Dag and B. Mirafzal, "On stability of islanded low-inertia microgrids," *2016 Clemson University Power Systems Conference (PSC)*, 2016, pp. 1-7.

[19] N. Jacobs *et al*., "Analysis of system and interoperability impact from securing communications for distributed energy resources," *2019 IEEE Power and Energy Conference at Illinois (PECI)*, Champaign, IL, USA, 2019, pp. 1-8.

[20] Q. Zhou, Z. Li, Q. Wu, and M. Shahidehpour, ''Two-stage load shedding for secondary control in hierarchical operation of islanded microgrids,'' *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3103–3111, May 2019.

[21] T. Caldognetto and P. Tenti, "Microgrids operation based on master–slave cooperative control," *IEEE J. Emerg. Sel. Topics Power Electron*, vol. 2, no. 4, pp. 1081-1088, Dec. 2014.

[22] X. Hou *et al*., "Distributed hierarchical control of AC microgrid operating in grid-connected, islanded and their transition modes," *IEEE Access*, vol. 6, pp. 77388-77401, 2018.

[23] "IEEE standard for smart energy profile application protocol," *IEEE Std 2030.5-2018 (Revision of IEEE Std 2030.5-2013)*, vol., no., pp.1-361, 21 Dec. 2018.

[24] I. Serban, S. Céspedes, C. Marinescu, C. A. Azurdia-Meza, J. S. Gomez, and D. S. Hueichapan, ''Communication requirements in microgrids: A practical survey,'' *IEEE Access*, vol. 8, pp. 47694–47712, 2020.

[25] S. Kumar, S. Islam, and A. Jolfaei, ''Microgrid communications—Protocols and standards,'' in *Variability, Scalability and Stability of Microgrids*. Jul. 2019, pp. 291–326. [Online]. Available: https://digitallibrary.theiet.org/content/books/10.1049/pbpo139e_ch9

[26] U. Sinha, A. A. Hadi, T. Faika and T. Kim, "Blockchain-based communication and data security framework for IoT-enabled micro solar inverters," *2019 IEEE CyberPELS (CyberPELS)*, Knoxville, TN, USA, 2019, pp. 1-5.

[27] R. S. de Carvalho and D. Saleem, "Recommended functionalities for improving cybersecurity of distributed energy resources," *2019 Resilience Week (RWS)*, San Antonio, TX, USA, 2019, pp. 226-231.

[28] M. R. Habibi, H. R. Baghaee, T. Dragiˇcevi´c and F. Blaabjerg, "Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks," *IEEE J. Emerg. Sel. Topics Power Electron.*

[29] M. R. Habibi, S. Sahoo, S. Rivera, T. Dragičević and F. Blaabjerg, "Decentralized coordinated cyber-attack detection and mitigation strategy in DC microgrids based on artificial neural networks," *IEEE J. Emerg. Sel. Topics Power Electron.*

[30] Y. He, G. J. Mendis and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505-2516, Sept. 2017.

[31] A. Mustafa, B. Poudel, A. Bidram and H. Modares, "Detection and mitigation of data manipulation attacks in AC microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2588-2603, May 2020.

[32] M. M. Rana, L. Li and S. W. Su, "Cyber attack protection and control of microgrids," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 2, pp. 602-609, Mar. 2018.

[33] L. Lu, H. J. Liu, H. Zhu and C. Chu, "Intrusion detection in distributed frequency control of isolated microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6502-6515, Nov. 2019.

[34] S. Zuo, O. A. Beg, F. L. Lewis and A. Davoudi, "Resilient networked AC microgrids under unbounded cyber attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3785-3794, Sept. 2020.

[35] S. Sahoo, Y. Yang and F. Blaabjerg, "Resilient synchronization strategy for AC microgrids under cyber attacks," *IEEE Trans. Power Electron*, vol. 36, no. 1, pp. 73-77, Jan. 2021.

[36] H. Zhang, B. Liu and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29641-29659, 2021.

[37] A. Ferdowsi and W. Saad, "Deep learning for signal authentication and security in massive internet-of-things systems," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1371-1387, Feb. 2019.

[38] J. Lamb and B. Mirafzal, "Grid-interactive cascaded h-bridge multilevel converter PQ plane operating region analysis," *IEEE Trans. Ind. Appl.*, vol. 53, no. 6, pp. 5744-5752, Nov.-Dec. 2017.

[39] J. Lamb and B. Mirafzal, "Active and reactive power operational region for grid-interactive cascaded h-bridge multilevel converters," *2016 IEEE Energy Conversion Congress and Exposition (ECCE)*, Milwaukee, WI, USA, 2016, pp. 1-6.