A Review of Cyber-Physical Security for Photovoltaic Systems

Jin Ye, *Senior Member, IEEE,* Annarita Giani, Ahmed Elasser, *Senior Member, IEEE,*
Sudip K. Mazumder, *Fellow, IEEE,* Chris Farnell, Homer Alan Mantooth, *Fellow, IEEE*
Taesic Kim, *Member, IEEE,* Jianzhe Liu, Bo Chen, *Member, IEEE,* Gab-Su Seo, *Senior Member, IEEE,*
Wenzhan Song, Mateo D. Roig Greidanus, Subham Sahoo, *Member, IEEE,*
Frede Blaabjerg, *Fellow, IEEE,* Jinan Zhang, Lulu Guo, Bohyun Ahn,
Mohammad B. Shadmand, Nanditha R. Gajanur, and Mohammad A. Abbaszada

***Abstract*—In this paper, the challenges and a future vision of the cyber-physical security of photovoltaic (PV) systems are discussed from a firmware, network, PV converter controls, and grid security perspective. The vulnerabilities of PV systems are investigated under a variety of cyber-attacks, ranging from data integrity attacks to software-based attacks. A success rate metric is designed to evaluate the impact and facilitate decision making. Model-based and data-driven methods for threat detection and mitigation are summarized. In addition, the blockchain technology that addresses cyber-attacks in software and cyber networks is described. Simulation and experimental results that show the impact of cyber-attacks at the converter (device) and grid (system) levels are presented. Finally, potential research opportunities are discussed for next-generation, cyber-secure power electronics systems. These opportunities include multi-scale controllability, self-/event-triggering control, artificial intelligence/machine learning, hot patching, and online security. As of today, this study will be one of the few comprehensive studies in this emerging and fast-growing area.**

Manuscript received XXXX XX, 2021; revised XXXX XX, 2021. This material is partially based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technologies Office Award Number DE-EE0009026. This work was authored in part by Argonne National Laboratory, managed by UChicago Argonne, LLC under contract DE-AC02-06CH11357; in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308.

J. Ye, L. Guo, and J. Zhang are with the Intelligent Power Electronics and Electric Machine Laboratory, University of Georgia, Athens, GA 30602, USA (e-mail: jin.ye@uga.edu, lulu.guo@uga.edu, jinan.zhang@uga.edu).

A. Giani and A. Elasser are with General Electric Research Center, Niskayuna, NY 12309, USA (e-mail: ahmed.elasser@ge.com).

S. K. Mazumder, M. D. Roig Greidanus, M. B. Shadmand, N. R. Gajanur, and M. A. Abbaszada are with the Electrical and Computer Engineering Department, University of Illinois at Chicago, Chicago, IL, 60607, USA (e-mail: mazumder@uic.edu, shadmand@uic.edu).

C. Farnell and H. A. Mantooth are with the Department of Electrical Engineering, University of Arkansas, Fayetteville, AR 72701 USA (e-mail: cfarnell@uark.edu; mantooth@uark.edu).

T. Kim and B. Ahn are with the Department of Electrical Engineering and Computer Science, Texas A&M University-Kingsville, Kingsville, TX 78363-8202 USA (e-mail: taesic.kim@tamuk.edu, bohyun.ahn@students.tamuk.edu).

J. Liu and B. Chen are with the Energy Systems Division, Argonne National Laboratory, Lemont, IL 60439 USA. (e-mail: jianzhe.liu@anl.gov, bo.chen@anl.gov)

G.-S. Seo is with the Power Systems Engineering Center, National Renewable Energy Laboratory, Golden, CO 80401 USA (e-mail:gabsu.seo@nrel.gov).

S. Sahoo and F. Blaabjerg are with the Department of Energy Technology, Aalborg University, 9220 Aalborg, Denmark (e-mail: sssa@et.aau.dk; fbl@et.aau.dk).

W. Song is with the Center for Cyber-Physical Systems, University of Georgia, Athens, GA 30602, USA (e-mail: wsong@uga.edu)

***Index Terms*—Cyber-physical security, firmware and network security, PV converter, cyber security assessment, detection and mitigation.**

I. Introduction

As the move towards smart grids and microgrids accelerates, protecting renewable energy assets, such as photovoltaic (PV) systems, against cyber-physical attacks and ensuring their security is becoming crucial to electric power grid reliability. To address the increasing cyber-security challenges associated with power electronics systems, the IEEE Power Electronics Society (PELS) has established a new Technical Committee on Design Methodologies. Existing studies on smart grid cybersecurity mostly focus on cyberattacks that impact grid reliability and availability rather than power electronics subsystems' performance and behavior.

This trend is due to the increasing penetration of the Internet-of-Things (IoT) enabled applications, such as connected Electric Vehicles (EVs) [1] and smart grids [2]. PV systems are differentiated from EVs and smart grid systems in terms of power levels (kWs to GWs), penetration levels, and the tight integration with many interfaces to the grid via grid-tied PV inverters and multiple sensors and communication hardware. PV systems are inherently intermittent, which leads to special challenges to determine "normal" vs. compromised behavior; thus, cybersecurity algorithms must be more carefully constructed and customized to detect attacks. It is easier for the attacker to hide in this more random signal environment. For instance, EV cybersecurity is best addressed through segmenting systems such as infotainment from vehicle operations, whereas PV cybersecurity and smart grids depend on communications to determine operational settings and control [2]. To contrast PV systems from the broader issue of smart grid cybersecurity, PV cybersecurity will focus on device-level through grid-level interactions, including communications, grid controls, and power conversion [2], whereas smart grid cybersecurity activities focus primarily on microgrid controllers and digital grid control and sensing. PV cybersecurity is a component of smart grid security that contributes to overall grid security. At the heart of PV systems is the power conversion device known as the PV solar inverter, a smart power electronics system that is responsible for interfacing with the grid.

Power electronics systems are becoming increasingly vulnerable to a variety of cyber threats, ranging from data integrity attacks (DIA) to denial of service (DOS) attacks. In addition, with the increasing number of distributed energy resources (DERs), such as PV and wind assets, along with their associated communication and smart technologies, the cyber-physical security of these renewable assets requires immediate attention [3], [4]. In a power electronics-based smart grid (PESG), grid-tied converters are remotely controlled by a plant controller and a supervisory control and data acquisition (SCADA) via power line communication (PLC), optical fiber, or wireless communications such as Zigbee, cellular (3G), and LTE (4G) [5], [6]. These communications and remote control capabilities will inevitably expand the cyber-attack surfaces, hence making PESGs vulnerable to cyber-physical attacks. These attacks include but are not limited to DIA and DOS. In addition, PESGs are susceptible to faults and degradation, such as power electronics device failures in open and-short circuit mode and passive component (e.g., capacitors) degradation.

As DER components' performance degrades over time, it can lead to abnormal PESG operating conditions, such as reactive power output imbalance, irregular power flow, and grid instabilities, such as sub-synchronous resonance, which might eventually cause the main grid to collapse or blackout. Recently, several operational issues due to improper firmware upgrades of PV solar plants have attracted increasing attention [7]. These operational issues resulted in abnormal inverter operations and faults. Examples include over and under voltage, volt/volt ampere reactive fluctuation, and unexpected power factor adjustments. In addition, networked power electronics systems are vulnerable to hacking from coordinated botnet via malicious software/process or via backdoor attacks in any of their compromised devices. For many safety-critical applications, if these threats are not detected at an early stage, they can lead to catastrophic failures and substantial economic losses.

In recent years, smart grid cyber-physical security has been extensively studied. In a recent study [2], security challenges and vulnerabilities in the control of grid-tied voltage source converters (VSCs) were discussed. Typical cyber-attacks that affect the operation of VSCs in microgrids, high-voltage DC (HVDC), static synchronous compensators (STATCOM), etc., are described in [2]. Cyber-attack assessment is discussed in [8], [9]. In [8], J. Zhang et al. proposed an assessment methodology for the cyber-attacks in a PESG. The proposed method uses attack scenarios such as DIAs to analyze their impacts on the stability and performance of smart grids. In [9], J. Zhang et al. analyzed the vulnerabilities in a PV farm and proposed machine learning and deep learning methods to detect cyber-attacks. Cyber-attack detection and diagnostics are discussed in [10]–[14]. [10] proposes a framework for the false-data injection attacks in a DC microgrid, in which invariants representing microgrid properties are extracted to detect cyber-attacks. [11] analyzes stealthly cyberattack mechanisms in DC microgrids and introduces a cooperative vulnerability factor based on the dynamic consensus algorithm in secondary controllers to detect cyber events. In [12], a novel high-dimensional data-driven method is used to detect cyberattacks and faults in electric power grids using a statistical leverage score and binary matrix factorization. [13] proposes a multilayer long short-term memory (LSTM) method to detect cyber threats in PV farms using point of common coupling (PCC) waveform data. [14] proposes an active detection method of deception attacks in microgrids. Attack-resilient controls are discussed in [15]–[17]. Considering the principle of heterogeneity raised by different types of sources, a novel resilient detection and mitigation methodology employing adaptive discord element is proposed for dc microgrids in [15]. [16] introduces a resilient control framework to deal with unbounded malicious attacks in electric power grids to ensure frequency and voltage stability. In [17], a time-delay recovery communication protocol is developed and simulation results demonstrate the efficacy of the method in multiarea frequency control of electric power grids. A cyberattack to PV systems that could falsify power generation by spoofing sensor data of the PV inverter is studied in [18]. Y. Isozaki et al. showed the impacts of cyber-attacks on the output power of PV farms in the distribution grid [19]. In addition to the emerging topic in the cyber-physical security of PV, the reliability and anomaly detection of PVs have been studied for many years. P. Zhang et al. presented a comprehensive review of the reliability assessment methods for power converters that includes capacitor aging, switching devices fault modes, and control firmware malfunction [20]. U. Jahn et al. proposed a reliability model to evaluate the performance of PV farms [21]. A. Golnas discussed the long-term performance of PV from the perspective of system operators [22]. To increase the fault detection accuracy, D. S. Pillai et al. summarized the advanced fault detection approaches for PV farms [23]. Although the cited literature work provides the technical foundation for PV farms cyber-security, their applicability is limited since cyber-attack impacts and surfaces are far more complex, so further studies are needed. There remain several major issues to be addressed and studied in detail: (1) Comprehensive cyber-attack models need to be developed to include cyber-attacks from different sources and locations, including firmware and network layers. (2) Existing detection and mitigation strategies mostly focus on cyber-attacks that adversely impact the functionality, stability, or maintenance cost of grid systems. (3) Cyber-attacks that compromise the performance of power electronics systems are not well addressed.

This paper describes the challenges, and proposes a cyber-physical security vision for a MW-scale PV farm. As of today, this study may be one of the few comprehensive studies in this emerging and fast-growing area. The main contributions of this paper are as follows:

- PV systems' cyber-physical security aspects: firmware and network, PV converter control, and grid security.
- PV systems' vulnerabilities investigations under a variety of cyber-attacks, ranging from data integrity to software-based attacks. A success rate metric is designed to evaluate the impact and facilitate decision making. Simulation and experimental results are provided to further analyze the cyber-attack impacts on both the converter (device) and grid (system) levels.
- Model-based and data-driven methods to detect and

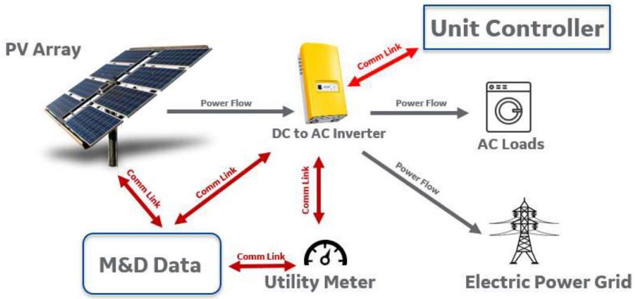


Fig. 1: A typical PV plant block diagram.

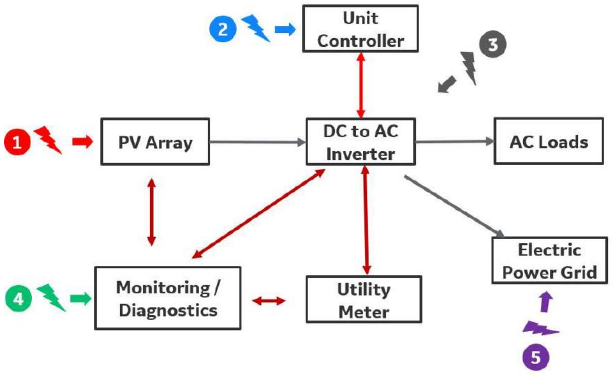


Fig. 2: PV plant potential cyber-attack points: i) physical, ii) inverter controller and algorithm, iii) supply chain, iv) monitoring and diagnostics platform, and v) grid.

mitigate cyber-attacks in PV farms.

- A blockchain algorithm to address cyber-attacks in software and cyber networks.
- Challenges and opportunities in designing next-generation cyber-secure power electronics systems, to provide readers with guidelines on future research directions.

II. Cyber-Physical Security in PV Farms

A. *Cyber-Physical Security in PV farms*

1) PV Farm Description: Figure 1 shows a typical PV array consisting of PV modules, a PV inverter, monitoring and diagnostics platform, and a utility meter. The PV array is connected to the grid and/or feeds AC loads via a grid-tied inverter. The grid-tied inverter performs maximum power point tracking (MPPT) on the overall PV array I/V characteristics and ensures that maximum power is extracted under various irradiance and temperature conditions. There are several MPPT algorithms that are used in commercial inverters [24]. When combined with battery energy storage systems, PV plants are used to charge the batteries during the day to dispatch it later. For solar-plus-storage plants, the ramp rate is the common algorithm that is used for energy management [25], [26].

A monitoring/diagnostic platform that acquires measurement data from various sensors that are deployed across the PV plant (e.g., module temperature, weather-related data, irradiance, power and energy data, and voltages and currents) is used to monitor the plant performance and diagnose any degradation, outages, and failures that might impact the plant reliability and availability. There are various levels of monitoring and diagnostics (M&D), granularity ranging from module, to inverter, to the plant level [27]. Data are acquired via a communication link between the PV array, the inverter, and the grid. A utility meter (for residential and commercial customers) tracks total energy production. With the increasing integration of large-scale PV farms into the power grid, the control methodologies and smart inverters allow PV farms to realize grid support services and respond to customer demand.

2) Cyber-Physical Security of PV farm: Cyber-physical attack points are identified as depicted in Figure 2.

- Attack number 1 is an actual physical attack on the hardware, such as tampering with the hardware (e.g., PV modules, combiner boxes, cables, inverters). The most prominent attacks that happened recently involve the stealing and the removal of PV modules for the purpose of reselling them [28], [29].
- Attack number 2 is an attack on the inverter controller and algorithms, and on the plant supervisory system (e.g., accessing and modifying the inverter controller software, accessing the unit controller to either shut down the plant or cause damage). Attacks on the PV inverter controls can occur at any moment through either the PV plant monitoring and diagnostics system, internet-enabled communications, or through the plant controller.
- Attack number 3 represents attacks that propagate throughout the supply chain (e.g., faulty electronic components, subpar analog, or digital parts). PV inverters are sophisticated electronics devices that use several advanced electronic components, such as a digital signal processor, micro controllers, and smart ASICs. These components can harbor malicious software that will corrupt inverter operation and cause it to fail.
- Attack number 4 targets the monitoring and diagnostics platform (e.g., data injection to mislead the operator, replay attack to mimic previous system operation, data integrity to falsify the sensor measurements). This type of attack is made possible by the increasing digitization of PV systems and the use of the IoT devices to communicate, send, and collect data from the PV plant. Increasingly, many inverter companies are prioritizing cybersecurity and are hardening their products [30], [31]. They are also providing end-to-end encryption of all information sent between their devices in the field as well as to their communication gateways and interfaces with the customer.
- Attack number 5 attacks are those that are directed at the grid and have the potential to significantly impact the plant operation and its overall safety (e.g., falsifying energy demand, disconnecting the grid from the plant). This attack is similar to attack number 2, but it propagates through the grid. Hackers can disconnect PV inverters from the grid by tripping the breakers or by inducing low-voltage, high-voltage, or zero-voltage conditions.

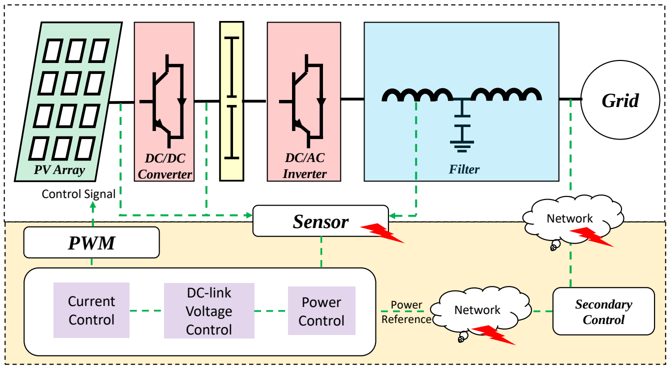


Fig. 3: Schematic diagram of a typical PV system.

B. Cyber-attack Model in PV Converter

Information technology (IT) cyber threats to confidentiality, integrity, and availability [32], [33], have been extensively studied. Similar to other cyber-physical systems, such as electric power grids and EVs, PV systems are vulnerable to similar cyber threats, including DIAs, DOS attacks, replay attacks, and stealthy attacks [1], [34]. In addition, an attack could falsify the power output of a PV converter by spoofing sensor data [18].

A typical PV converter and associated vulnerabilities are shown in Figure 3. The measured data from sensors and power control reference are expressed as $Y(t) = [I_{dc}(t), U_{dc}(t), I_f(t), U_c(t), I_g(t)]^T$, $S(t) = [P^*(t), Q^*(t)]^T$. Where I_f is the inverter filter-side inductor current; U_c is the filter capacitor voltage; and I_g is the grid side current. I_{dc} is the PV array output current. U_{dc} is the DC-link voltage. The cyber-attack model can be expressed as follows:

$$\begin{aligned} Y(t) &= \alpha * Y_F(t) + \beta * Y_0(t - t_{delay}) \\ S(t) &= \gamma * S_F(t) + \phi * S_0(t - t_{delay}) \end{aligned} \tag{1}$$

where Y, S are the compromised data vectors that are eventually the input to the power converter controller; Y_0, S_0 are the original measurements; Y_F, S_F are the biased vectors, which can be independent or a function of Y_0; α and γ are multiplicative factor matrices that define the weight of the attack vectors; β and ϕ are multiplicative factor matrices that define the weight of the real vectors; and t_{delay} is the time delay that is inherent in communication systems and/or caused by cyber-attacks. In this definition, α is the multiplicative factor matrix, and it can be expressed as an 11×11 matrix:

$$\alpha = diag\ [\alpha_{ipv}, \alpha_{udc}, \alpha_{il_{1\times3}}, \alpha_{uc_{1\times3}}, \alpha_{ig_{1\times3}}]. \tag{2}$$

where, β, γ, ϕ could be formed based on the definition of α. The attack duration is denoted as $t_a = [t_s, t_e]$, where t_s and t_e represent the start and end time of the attack. Typical cyber-attacks are described as follows. To exhibit and analyze the impact of cyber-attacks on a PV farm, seven sets of two-stage PV inverters are simulated in an Opal-RT® real-time test bed. Opal-RT is used for control algorithm validation. MATLAB® has been integrated with Opal-RT using the software module RT-LAB™ within Opal-RT. To achieve real-time simulation, C code generated by RT-LAB is executed on OPAL-RT to simulate the dynamic performance of the power electronics components. Detailed information on the testbed and PV farm are shown in Tables I and II, respectively.

TABLE I: PV inverter parameters

Rated Power	125 kW	DC-Link voltage	1500 V
L_{filter}	3.5 mH	L_{grid}	1.8 mH
C_{filter}	7.2 μF	Grid Voltage	480 V

1) Data Integrity Attack: DIAs can directly falsify measurements of the sensor or power references [9]. Considering the attack model in equation (1), the multiplicative factors β and ϕ determine the scaling attack impact on the PV farm [36]. Notice that the strength of the cyber-attacks could vary owing to the elements in the attack vector [α, β]. As shown in Figure 4, both single- and three-phase DIAs on the inverter filter-side inductor current, I_f, beginning at the 15s time instant, affect the operation of PV Converter #1 (PV #1). Afterwards, the same disturbance at the power generation level of the PV farm appears under single- and three-phase DIAs. Compared to the unbalanced current injected by a single-phase attack shown in Figure 4(a, b), a three-phase DIA exerts a more serious impact on inverter side current and the capacitor voltage of PV #1. As shown in Figure 4(c), the output currents' frequency at the PCC is affected due to DIAs, which attests to the strength of two DIAs. Based on the PCC voltage waveform, the two attacks have a similar influence on the PCC voltage—the PCC voltage frequency shows an obvious difference between the single- and three-phase DIAs, as shown in Figure 4(c). Compared to the distortion of the PCC current, the DIAs' impact on the PCC voltage is more limited.

2) DOS Attack: A DOS attack is a typical IT attack that shuts down the network by overwhelming it with traffic [37]. This type of attack makes the sensor measurements or the power references inaccessible. DOS attacks work by compromising a PV plant sensor and delaying the measurement data so that the plant controller cannot acquire the PV inverter feedback at the appropriate time. Figure 5(a) shows the effects of a DOS attack on the inverter filter-side inductor current, I_f, of PV #1,—its delay time is increased by 0.11s. The disturbance appears in the PV output current, filter capacitor voltage, and PV power output after 15s of the onset of the attack. Although there is no obvious variation in the magnitude of the PCC voltage, the frequency of the PCC current and voltage exhibits a discernible difference when compared to the normal condition, as shown in Figure 5(c). Compared with DIAs, there is a different frequency pattern of PCC current and voltage under DOS attack.

3) Replay Attack: Replay attacks, also called playback attacks, repeat, or delay the sensor data or control command to the PV farm [38]. First, the hackers save the data in the communication network and then maliciously falsify sensor data by re-injecting the saved data. This attack cannot be detected by only monitoring the sensor data or by control command, but it can disturb or damage the PV farm operation. Replay attacks can be modeled as in equation (1) by substituting $Y(t)$ and $S(t)$ with the previously saved data by the hackers. The impact of a replay attack on PV #1 and the PV farm

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2021.3111728, IEEE Journal of Emerging and Selected Topics in Power Electronics

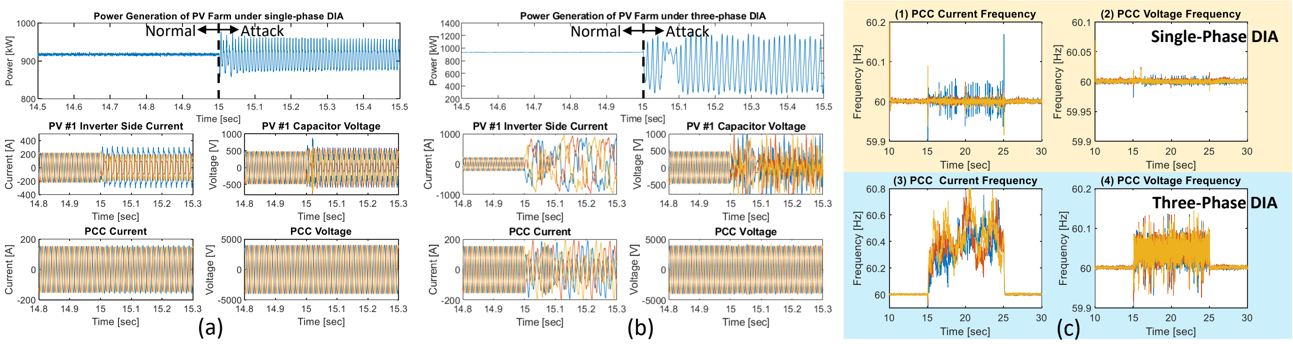


Fig. 4: DIAs' impact on PV Converter #1 (PV #1) and PV farm [35].

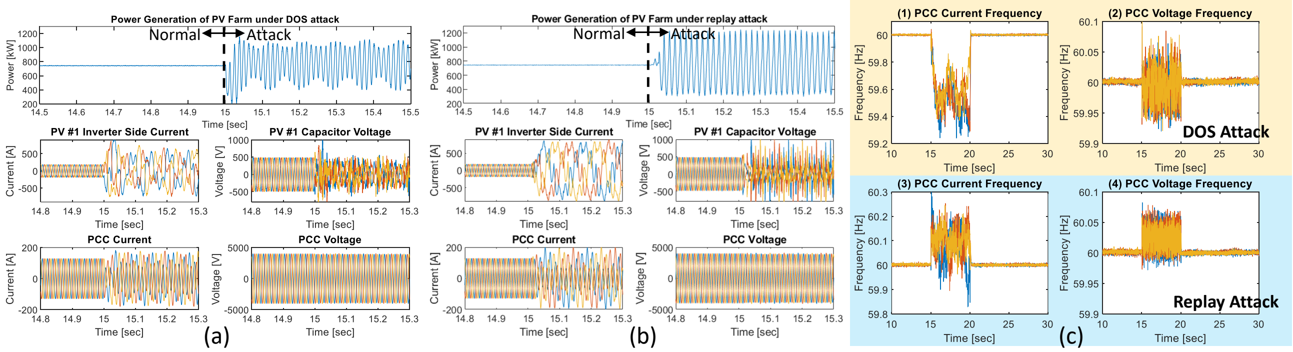


Fig. 5: Impact of DOS attack and replay attack on PV Converter #1 and PV farm [35].

TABLE II: OPAL-RT OP5700 Specifications

CPU	Intel(R) Xeon E5, 8 cores, 3.2 GHz, 20M Cache
Installed Memory (RAM)	8.0 GB
Motherboard	X10DRL-I Supermicro Motherboard Dual Intel Xeon Processor

are shown in Figure 5(b, c). The mismatch between the saved data and the real measurements degrades the controller performance of PV converter #1. As with DIA and DOS attacks, the frequency of the PCC voltage and current shows an obvious variation during the attack time. After a replay attack is implemented at the 15s time instant, a slow change in the PV power output is observed, which is a unique feature for this type of attack.

4) Stealthy Attack: A stealthy attack depends on the skill and professional knowledge of the hacker. An attacker could constantly generate a negative impact on the PV system operation while being undetected. This type of attack could be more destructive to power electronics-based systems than traditional power systems, by taking advantage of their low-inertia property; hence, an attacker can cause more harm to a power electronics-based system while momentarily staying undetected. C. Zhao et al. provided the analysis of stealthy attacks in a smart grid under a well-developed consensus-based protocol [39]. M. Esmalifalak et al. proposed two machine learning methodologies for the detection of stealthy attacks in a power grid [40]. The time it takes to detect stealthy attacks on control systems highly depends on the complexity of the attack stemming from the attackers' knowledge of a power system model. S. Harshbarger et al. provide an analysis on how uncertainty in the power grid model may impact the detection of stealthy attacks [41].

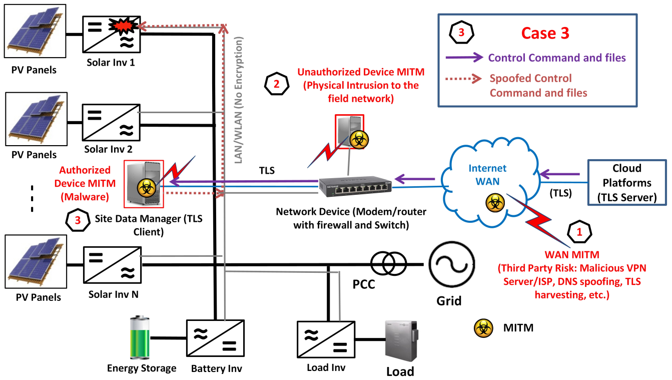

3
Case 3
Control Command and files
Spoofed Control Command and files
PV Panels
Solar Inv 1
Solar Inv 2
Solar Inv N
LAN/WLAN (No Encryption)
2
Unauthorized Device MITM (Physical Intrusion to the field network)
Authorized Device MITM (Malware)
3
Site Data Manager (TLS Client)
TLS
Network Device (Modem/router with firewall and Switch)
Internet WAN
(TLS)
Cloud Platforms (TLS Server)
1
WAN MITM (Third Party Risk: Malicious VPN Server/ISP, DNS spoofing, TLS harvesting, etc.)
PCC
Grid
MITM
Energy Storage
Battery Inv
Load Inv
Load

Fig. 6: Cases of MITM attack in a PV system that modify in-transit data from cloud platforms.

C. Network and Software/Firmware Security in PV Farm

The cybersecurity of PV systems still relies on network-based security postures, such as firewall rules, authentication of users, and the encryption of communication-based on transport layer security (TLS) [42], [43]; however, security entails a much larger scope than current network-based security methods. Encryption only ensures that the encrypted data cannot be understood; therefore, encrypted spoofed messages/malware easily bypass firewalls. Furthermore, current field network protocols (e.g., Modbus TCP/RTU and SunSpec Modbus) in PV farms have no or weak security measures. Moreover, human risks always exist, which threatens users' passwords and malware installations [44]. Attackers use the exposed vulnerabilities of PV systems. A typical network attack is a (D)DoS attack attempting to disrupt a network rendering the controller unavailable to receive data or commands. Attackers in these types of attacks typically flood web servers, systems or networks with traffic that overwhelms target networks with bogus traffic, making it difficult for victim inverters or a PV system control server to operate normally [45]. As described in Section II.B, the external control commands, S(t), and PV system sensor data delivered to the inverter controller through communications (i.e., in-transit data) could be modified by network attacks, such as man-in-the-middle (MITM) attacks [46]–[48]. Fig. 6 shows three potential MITM attack cases that can change in-transit data in a PV system [49]: 1) a wide-area network (WAN) MITM, 2) an unauthorized device MITM; and 3) an authorized device MITM. WAN MITM attacks could be caused by a third party, such as a virtual private network (VPN) provider, a domain name server (DNS), or an internet service provider (ISP)). Since the security of the third party is outside the security perimeter of the PV system, it is hard to validate data passed by the malicious third party or breached third party by attackers. Although people consider that TLS is currently secure, advanced attacks such as TLS harvesting can break TLS (e.g., stealing session key logs). Second, an unauthorized MITM device will be physically located and connected to the local area network (LAN). Field network protocols without strong authentication and encryption are vulnerable to this type of MITM attack. Note that most MITM attack detection in PV systems applied this attack scenario. Due to the malware injection attacks, the authorized devices can be a MITM attack devices. As shown in Fig. 6, a site data manager is an aggregator and a gateway in a PV system acting as a major middleman between the inverters and the cloud. The encrypted TLS data are decrypted and converted to the local network protocols such as Modbus TCP in the site data manager; therefore, a malicious site data manager can easily make MITM attacks although this device is authenticated and authorized in the current PV system security perimeter such as firewall rules and encryption-based security controls. Although, the site data manager will be a critical target device from the attacker's perspective, compromised inverters or operational technology network devices can also create MITM attacks. Attackers also exploit software/firmware update events to create cyber-attacks [50], which can directly or indirectly target the inverter controller, as described in Section II.B. The attack surface of software/firmware in a solar farm control center and smart inverters includes three major attack points [51]: 1) Remote vendor access via the regular software update and maintenance; 2) Operator access via a remote user interface; and 3) Physical access via USB flash drives or LAN or reverse engineering/side-channel attacks. Advanced attackers such as advanced persistent threat (APT) groups [52] and insider threats (e.g., disgruntled employees or malicious insiders [53]) can disguise as vendors or authorized users to modify software or inject malware (e.g., backdoor, Trojan horses, viruses, worms, ransomware, and rootkits [54]). Attackers who can access the inverter 'firmware enable' function can modify the behavior of the inverter and lead to malfunction or performance degradation (i.e., stealthy attacks that avoid being detected by intrusion detection systems (IDSs)). For example, the sensor matrix, Y(t), which is generated by embedded sensors in the inverter, can be altered by injecting malicious code in the inverter firmware through flash memory data modification in an inverter control card [55] or over-the-air update [51]. The software/firmware and in-transit data modifications will occur once the chains of cyber-attacks are successful. Examples of such cyber-attacks are: malware backdoor injection through the supply chain [56], eavesdropping for snipping credential data, spoofing through security certificates to gain unauthorized access, least-privilege violations to access unauthorized services, and brute-force credentials and side-channel attacks to guess the password or a security key [57]. Additional information on adversarial tactics and techniques based on real-world attacks is found in MITRE's ATT&CK for Industrial Control Systems (ICS) [58].

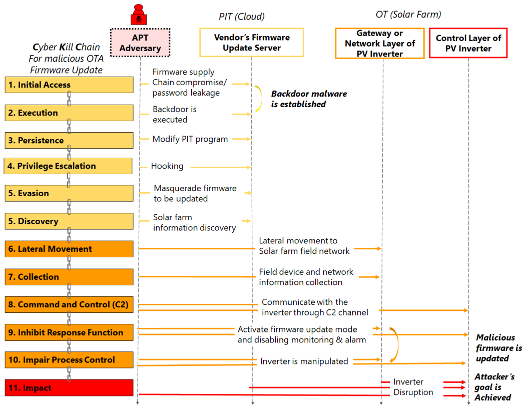

APT Adversary
PIT (Cloud)
OT (Solar Farm)
Vendor's Firmware Update Server
Gateway or Network Layer of PV Inverter
Control Layer of PV Inverter
Cyber Kill Chain For malicious OTA Firmware Update
1. Initial Access
2. Execution
3. Persistence
4. Privilege Escalation
5. Evasion
5. Discovery
6. Lateral Movement
7. Collection
8. Command and Control (C2)
9. Inhibit Response Function
10. Impair Process Control
11. Impact
Firmware supply Chain compromise/ password leakage
Backdoor is executed
Backdoor malware is established
Modify PIT program
Hooking
Masquerade firmware to be updated
Solar farm information discovery
Lateral movement to Solar farm field network
Field device and network information collection
Communicate with the inverter through C2 channel
Activate firmware update mode and disabling monitoring & alarm
Malicious firmware is updated
Inverter is manipulated
Inverter Disruption
Attacker's goal is Achieved

Fig. 7: A cyber kill chain model.

Fig. 7 illustrates a scenario of a firmware attack targeting to disrupt a PV inverter, where the cyber kill chain (CKC) model is designed based on ATT&CK for ICS framework. An adversary is trying to access a platform information technology (PIT) system (e.g., a vendor providing firmware update server) by using the supply chain of software developed by a 3rd vendor or old employee's weak passwords, or a VPN password leakage (1. Initial Access). A backdoor malware is installed in the server (2. Execution). The adversary is trying to maintain foothold to continuously access and explore the server (3. Persistence). The adversary is trying to gain higher-level permission (4. Privilege Escalation). Adversaries may use masquerading to disguise a malicious code/modification in the firmware to be updated to avoid operator and engineer suspicion (5. Evasion). Afterwards, the field side PV system information in the PIT is gathered by the adversary (6. Discovery). The adversary can freely access the solar farm via valid remote access pathways (7. Lateral Movement). The adversary is trying to gather data on the solar farm domain (8. Collection). The adversary is trying to communicate with and control a target PV inverter through the authorized command and control channel (9. Command and Control). The adversary activates the firmware update mode and disables the monitoring and alarm functions on the inverter (10. Inhibit Response Function). The malicious firmware is updated to manipulate the inverter (11. Impair Process Control). Finally, the adversary is trying to manipulate, interrupt, or destroy the inverter (12. Impact).

III. Cyber-Physical Security Assessment in Photovoltaic Farms

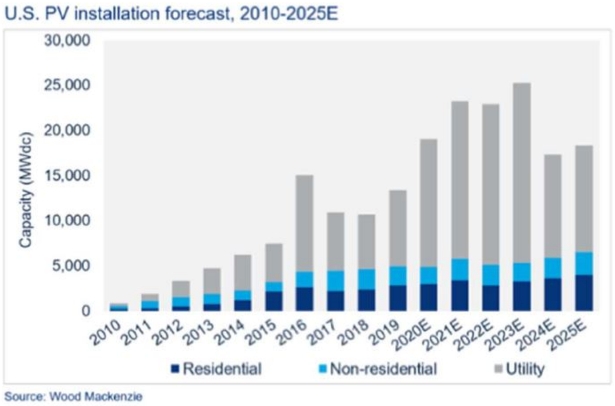
In this section, the cyber-physical security assessment in PV farms is introduced with real-world case studies. Furthermore, a success rate metric is proposed for cyber-attack assessments in PV farms.

A. Attack Consequences and Assessment for PV Farm

A key part of a cybersecurity evaluation is to assess the impact of a cyber-attack, on the equipment, services, and plant mission. The consequences of such attacks directly affect the attacked assets and propagate through mission and system dependencies. Previous efforts have been focused on proposing and devising methods for quantifying the impact of cyber-attacks. As an example, Jakobson [59] proposed a four steps conceptual framework and a method for assessing the impact that cyber-attacks have on a given asset. These four steps are: 1) Attack Point Detection, which identifies the exact target of an attack and the vulnerabilities it may exploit. 2) Direct Cyber-Attack Impact Assessment, which determines the direct impact of the cyber-attack on the asset that it is targeting. 3) Propagation of the Cyber-Attack throughout the system dependencies. 4) Impact Assessment on the high-level missions based on asset dependency relationships derived by the logical mission models. Giani et al. proposed, analyzed, and quantified metrics for assessment of data integrity attacks on the smart grid [60]. These are a class of cyber-attacks that compromise grid information that is processed by grid operators. The latter may include energy meter readings of injected power at remote generators, power flows in transmission lines, and protective relays' status. Some of these cyber-attack consequences are: 1) Financial losses from sub-optimal economic dispatch [61] (e.g., altering cost of electricity) to service loads, 2) Robustness/resiliency losses (e.g., changing on/off status of power lines) from placing the grid at operating points that are at greater risk from contingencies and 3) Systemic losses (e.g., shifting loads to nearby elements of the system) resulting from cascading failures induced by poor operational choices. Liu et al. studies the impact of cyber-attacks on microgrids, and specifically on PV and energy storage systems (ESS) controls [62].

B. Case Study

Cyber-attacks on PV systems are real. On March 5th, 2019 sPower, a Utah-based provider of solar and wind energy was a victim of a DOS attack [64]. The vulnerability exploited was an unpatched firewall and the attack caused the power grid operator to become disconnected from its power generation station from 9 a.m. until 7 p.m. local time [64]. Teymouri et al. investigated the impact of cyber-attacks on a distribution grid (with a PV plant that provides reactive power) with a focus on voltage regulation [65]. They showed how the modification of grid measurements by the attackers affects the dynamics and reactive power injection capability of the PV inverter. The master and local controller are vulnerable assets that can be modified by an external source, hence impacting the overall distribution grid. These types of attacks can continue undetected for a long time since they do not violate any detection constraint [65]. Isozaki et al. also addressed cyber-attack on distribution power grids and specifically on voltage regulation. They demonstrated that if voltage measurements are falsified by an attacker, voltage violation can occur in the system [19]. They also showed that with the appropriate use of a detection algorithm, the damage can be limited.



Source: Wood Mackenzie

Fig. 8: U.S. solar PV deployment forecast [63].

The consequences of cyber-attacks on PV plants may vary depending on a host of factors. One such factor is the type of installation (i.e., residential, commercial, and utility). Figure 8 shows the growth trajectory of PV in the United States; hence it is important to address cyber-attacks and prevent attackers from disrupting the Nation's power grid. Based on the scale of the PV plant farm, i.e., residential, commercial, or utility, the consequences can be different, as shown in Table III. A residential PV system can be part of a microgrid, and it can also include energy storage, but it is generally grid-tied. Power loss is the main consequence of an attack, which translates into monetary loss to the consumer. Additional consequences are damage to the equipment and, in extreme cases, loss of the components. Privacy is another critical issue in the cybersecurity of residential PV systems, as the usage of the PV-generated power reflects the behavior of the users which can be exploited to launch additional attacks. Commercial PV systems which are used by small, medium, and large businesses, are used to offset energy costs as well as participate in the energy trading market. They are generally paired with monitoring and control devices (e.g., unit controllers, Phasor Measurement Units (PMUs), etc.) and are equipped with rapid shutdown solutions to eliminate shock hazards for emergency responders. Attacks on commercial PV systems may lead to damages to daily operations, system failure, disruptions to grid services, and ultimately, to damages at the grid level. For utility PV systems that are used by electric utilities and energy providers,

TABLE III: Impacts of cyberattacks on residential, commercial, and utility PV systems.

Residential(3-10kW)	**Commercial(10kW-2MW)**	**Utility(>2MW)**
Power loss/Monetary loss	Damage to overall commercial operation	Power/Monetary loss
Equipment/Component damage	System failure	Grid instability
Loss of the unit itself	Damage to grid services	Loss of the PV solar farm
Privacy	Domino effect, propagation to other systems in the grid	Power generation cost fluctuation

the consequences of cyber-attacks can be far-reaching and lead to significant monetary losses, disruption of services to customers, and ultimately to grid instability and blackouts. Even locally and limited targeted attacks on a PV utility farm can cause a fluctuation in the cost of electric power generation, therefore, increasing the cost of electricity and denying service to customers.

C. Success Rate Metrics

Metrics are tools that are designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data [66]. Many existing approaches compute Security Risks as Threat x Vulnerability x Impact, but this definition is limited since it is very difficult to quantify each value [67]. Important elements involved in quantifying metrics are: 1) Asset value, which is defined by plant size, utilization, reliability, and availability; 2) Cost of downtime which is the result of losing the PV plant due to a cyber-attack; and 3) Security costs required to prevent, detect, respond, and mitigate the impact of a cyber-attack.

Based on the published and public domain literature and research, the following metrics to measure the success rate of an attack are proposed, as shown in Table IV. These metrics address the effectiveness of a cybersecurity response strategy and solution as a function of mitigation effectiveness, detection rate, neutralization power, consequences avoided, and solution cost. Mitigation effectiveness measures the efficacy of the proposed solution to mitigate the effect of the cyber-attack. Detection Rate measures the quality of the solution to detect cyber-attacks. Neutralization Speed measures the speed by which the proposed solution neutralizes the cyber-attack. Consequences Avoided measures the value of the cyber-attack impact on the PV plant if the cyber-attack had taken place and succeeded in disrupting the system. Solution Cost measures the cost of implementing and deploying a security solution to avoid further cyber-attacks. Total Solution Success measures the overall cyber-security solution power.

Table IV shows a specific example in which the detection rate is high, the neutralization power is low, and the rest of the metrics are rated medium. The solution success is a weighted average that depends on the weights assigned to the various metrics and on how the customer perceives them based on their mission profile. For Table IV and with equally distributed weights, the solution success is rated 3 or medium. When a specific weight is assigned to each aspect of the solution, the total solution success is defined as:

TABLE IV: Proposed three-level cyber security metrics and an example of a cyber attack. Level 1 is Low impact, Level 2 is Medium impact and Level 3 is High impact.

Metrics	Weight	1-L	3-M	9-H
a_1: Mitigation Effectiveness	p_1		×	
a_2: Detection Rate	p_2			×
a_3: Neutralization Speed	p_3	×		
a_4: Consequences Avoided	p_4		×	
a_5: Solution Cost	p_5		×	
a_0: Total Solution Success			×	

$$a_0 = \frac{\sum_{i=1}^{n} p_i a_i}{n} \tag{3}$$

where p_i is an integer that represents the weight associated with the aspect a_i of the solution methodology; and n is the total number of metrics. As with any other asset, the cybersecurity of PV systems involves a variety of aspects and poses several questions and challenges that need to be addressed when selecting and developing a security strategy.

The weight factors depend on the type of operation that the PV plant supports. For example, in an environment where daily operations rely exclusively on the power generated by the PV farm, the consequences of a cyber-attack are significant, and the weight associated with “Consequences Avoided” is high, 10 on a scale from 1 to 10. Under the same circumstances, the weight associated with “Solution Cost” is low to moderate, 3 to 5 since these types of installations prioritize reliability and continuity of service over cost. When service restoration is prioritized such as for critical assets like data centers or medical facilities, the weight associated with “Neutralization Speed” is high. In a situation such as a large PV farm, where the attack might propagate to other devices, detecting the attack is a priority and the weight associated with the “Detection Rate” becomes significant. In all cases mitigating the effect of the attack is important to limit the damages to the customers, the facilities and the equipment, hence the weight associated with “Mitigation Effectiveness” is generally high.

IV. Overview of Detection and Mitigation Methodology

To address the cyber-physical security issue of PV farms, this section presents cyber-attack detection and mitigation methodologies including model-based cyber-attack detection, data-driven cyber-attack detection, and network and firmware security detection and mitigation.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2021.3111728, IEEE Journal of Emerging and Selected Topics in Power Electronics

A. Model-based Cyber-Attack Detection for Control Security in PV Farm

Cyber-attacks can affect the control system in a PV farm by corrupting the sensor measurements received by the controller and the control decisions sent to the actuators. Model-based cyber-attack detection methods seek to use physics-based models that are meant to emulate systems under no-fault conditions to compare with actual system measurements to recognize anomalies by uncovering inconsistencies between the modeled and actual performance [68]. This inconsistency is evaluated against a residual threshold.

We show below a general model of a PV farm whose control system is under cyber-attack:

$$\dot{x} = f(x, u_a) + \omega_1, \tag{4a}$$

$$y = h(x, u) + \omega_2, \tag{4b}$$

$$u = g(y_a) + \omega_3, \tag{4c}$$

$$y_a = y + \alpha_1, \quad u_a = u + \alpha_2, \tag{4d}$$

where x, y, u represent the system state, output, and input variables; f, h, and g represent some potentially nonlinear equations describing system dynamics, measurement equation, and control design; ω_1, ω_2, and ω_3 represent the system disturbances; α_1 and α_2 represent the attacks signals on measurement information and the control decisions; and u_a and y_a are the corrupted input and output information. Notice that (4a) can model both DOS and faulty data injection attacks. A variety of model-based cyber-attack detection methods have been developed.

First, bad input data detection methods have been developed for cyber-attack detection [69]. Bad data analysis methods are initially developed for power system state estimation to remove the measurement or topological errors in input data [70]. A variety of methods have been developed for bad data detection [71]–[74], including residual normalization method, geometric method, sensitivity analysis, and geometric approaches. They have good performance if statistics about the errors of the data are known. Notice that the power output from individual PV inverters and the power flows within a PV system have a huge impact on the overall power generation output. They are closely monitored by the PV system SCADA. The state estimation based attack detection methods have a wide range of applications by leveraging the existing SCADA measurement and monitoring capabilities. We exemplify the main idea by using the following classic weighted least-square (WLS) problem:

$$\min_{x} \quad (y_a - h(x, u_a))^\top W (y_a - h(x, u_a)), \tag{5}$$

where W is a weight matrix usually obtained through measurement error statistics [75]. Suppose the solution of (5) is $\hat{x}$; it is considered as an estimation of the system states based on received system measurements y_a. Let r be a residual defined as follows,

$$r = y_a - h(\hat{x}, u_a). \tag{6}$$

Let $||\cdot||$ represent Euclidean norm. It is assumed that the estimated states obtained based on the corrupted information cannot fit the physics-based model very well. Hence, regarding $||r||$, a larger than normal value would be generated when there is presence of attacks. Based on this idea, a residual threshold is often determined prior to deployment to test $||r||$. An anomaly caused by cyber-attacks can be detected when the threshold is passed. The method leverages the mature power system state estimation approaches and is amenable to applications.

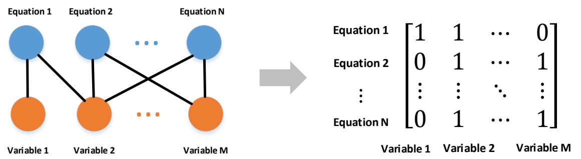


Fig. 9: Bipartie diagram and structural representation

Similarly, dynamic state estimation methods like the Luenberger observer method [76] for linear systems and the Generalized Kalman filter method [77] for nonlinear systems have been developed for cyber-attack detection as well. PV systems have rich dynamics arising from the integration of PV inverters regulated under various control strategies. When the controllers are marred by cyber-attacks, the system dynamical behaviors will then deviate from the normal operational conditions. The basic idea of using the dynamical state estimation based methods is to find the estimated system model and output (often defined as $\hat{y}$) to be compared with the received readings to ascertain the presence of cyber-attacks: If the difference between $\hat{y}$ and y_a is "significant enough", an anomaly is believed to be found. This comparison is usually conducted using χ^2 detectors [37]. The χ^2 detector compares the statistical characteristics of the obtained residual with the normal case, for example, it calculates the following value:

$$g = r^\top Q^{-1} r, \tag{7}$$

where Q is the covariance matrix of r and g a scalar. When r is of a given distribution, g may conform to a fixed distribution correspondingly (e.g., if r is Gaussian distributed then g is χ^2 distributed).

The third category of model-based cyber-attack detection methods is based on FDI methods [78]–[80]. Such methods usually construct state observers or use parity equations to generate residuals for attack detection purposes. FDI-based methods usually conduct a detectability analysis aiming to determine whether a subset of system equations can be found such that it contains enough data redundancy to generate the specific residuals to detect certain attacks. The detectability analysis method is usually conducted using graph theory methods. For example, a bipartisan diagram is usually constructed to reveal the structure of a system as shown in Fig. 9. It can be observed that with N equations and M variables, an $N \times M$ binary matrix can be constructed such that if variable j exists in equation i the element on the i-th row and j-th column is one, which is otherwise zero. From the binary matrix, graph theory methods like the Dulmage-Mendelsohn decomposition method can be applied to obtain the subset to find residuals.

Although the above-mentioned detection methods work well in many applications, in the context of coordinated cyber-attacks they have potential critical loopholes that might prevent

TABLE V: Waveform detection results $Acc_{(\cdot)}$=[ANN, LSTM, CNN] (%, 20kHz, Epoch=300)

Accuracy	$N_w = 400$	$N_w = 600$	$N_w = 800$	$N_w = 1000$
Acc_{det}	[91.18, 98.49, 98.13]	[92.53, 98.82, 99.36]	[93.09, 99.53, 97.96]	[91.85, 97.80, 99.44]
Acc_{nom}	[88.91, 99.63, 98.37]	[89.45, 99.93, 98.89]	[92.36, 99.78, 99.49]	[85.87, 97.69, 99.14]
Acc_{dia}	[86.76, 96.69, 91.17]	[83.43, 97.63, 98.37]	[83.69, 99.23, 89.18]	[86.08, 97.30, 97.73]
Acc_{replay}	[87.11, 98.67, 96.00]	[81.20, 98.00, 95.60]	[89.67, 93.27, 95.52]	[88.12, 98.36, 96.72]
Acc_{fault}	[99.54, 99.77, 99.77]	[99.75, 100.0, 99.78]	[99.79, 100.0, 99.78]	[99.76, 100.0, 100.0]

them from performing as expected [11]. For example, in (5), it can be seen that the corrupted control decisions u_a are included in the cost function as well. If u_a is maliciously chosen such that r is placed below the threshold, the method then fails to spot cyber-attacks anymore.

Another class of methods that could potentially tackle the issue is based on Hypothesis Testing. The basic idea behind these methods is to compute the conditional probability of the existence of a cyber-attack for two (or more) hypothetical conditions, i.e., 1) the attack is absent or 2) there exists a smart adversary that deliberates cyber-attacks with the perfect system information [81]. The methods have been widely used to monitor a group of sensors [82], a subset of which are under attack and a system monitor needs to locate the corrupted sensors based on all the received measurements. As discussed above, a PV system has a large amount of sensors and is usually equipped with a SCADA for monitoring purposes. Hence, the aforementioned scenario could happen, and exhibit considerable challenges for PV system operations. The Hypothetical Testing based methods usually use the flexible tools from robust optimizations, like minimax or game-theoretic approaches, to describe the competition between the system monitor and the adversary, in which the system monitor decides the probability of an attack in the “worst-case” that an adversary could incite.

B. Data-driven Cyber-Attack Detection for Control Security in PV Farm

In recent years, data-driven methodologies that do not require physical models have gained continued interest in smart grid applications. There are many different data-driven methods, including stacked auto-encoder (SAE) [83], reinforcement learning (RL) [84], vector autoregressive model (VAR) [85], dynamic Bayesian networks (DBN) [86], deep neural networks (DNN) [87], LSTM [88], PCA reconstruction (PCA) [89], cumulative sum (CUSUM) [90], influential point selection [91], and support vector machine (SVM) [40]. Specifically, in power system fields, data-driven methodologies are used to detect various cyber-attacks which falsify the market and system operation. In [92], the authors proposed an SAE- based deep learning method to detect cyber threats in the state estimation of SCADA. In power markets, the CUSUM statistical model was used to detect cyber threats [90]. In [93], the authors proposed an online cyber attack detection methodology using reinforcement learning. A distributed SVM was designed to detect the stealthy false data injection attacks in smart grids [40]. In [94], the authors improved the performance of the supervised learning techniques algorithm with heuristic feature selection. A deep belief network was designed to detect the false injection attacks in real-time using captured features in the historical measurement data [95]. In [96], the authors designed a cyber anomaly detector using a convolutional neural network (CNN) and LSTM. In addition to supervised learning that requires a large amount of data in training, unsupervised learning is increasingly popular, which can cluster data into different classes according to a certain feature. Unsupervised anomaly detection using a statistical correlation between measurements was proposed in [86].

While there is extensive work on data-driven methods in power grids, data-driven detection for PV security is in its early stage. As described above, in PV systems, both device-level and system-level controllers are vulnerable to cyber-attacks. In [12], we proposed a statistical data-driven approach to detect and diagnose a variety of cyber-physical threats for distribution systems with PV farms, including cyber-attacks on the solar inverter controller, cyber-attacks on relays/switches, and other faults (e.g., short circuit faults). Considering cyber-attack impacts on two-stage PV converters, a deep-sequence-learning-based detection and diagnosis was proposed for data integrity attacks in PV systems [13]. For comparison, [13] shows a comparison and evaluation of classic data-driven methods, including K-nearest neighbor (KNN), decision tree (DT), SVM, artificial neural network (ANN), and CNN. In addition, we developed machine learning methods to detect cyber attacks that can lead to the PV inverter performance degradation through the use of micro-PMU data at the PCC [97].

In general, most learning-based methods identify the anomaly in the system based on the monitoring data. Considering the impact of noise on measurements, the discrepancy between falsified data and estimated data is calculated in different feature spaces. Besides cyber-attack detection, the data-driven methods are used to distinguish from normal conditions, DIA, replay attacks and physical faults. A comparison study using PCC waveform data is conducted in the real-time testbed [35] to diagnose the type of attacks/faults in the PV farm. TABLE. V shows the Artificial Neural Networks (ANN), LSTM, and CNN. LSTM and CNN exhibit a better performance in this case study. ANN is a feed-forward neural network, which cannot capture sequential information in time series data. Instead, CNN utilizes the convolutional kernels to extract features of measurement data. Compared to ANN, CNN is more accurate using a higher number of layers. In most cases, LSTM achieves a higher successful detection rate. This is because LSTM as a special case of Recurrent Neural Networks (RNN) is capable of learning long-term dependencies. Thus, its model is more effective at capturing long-term temporal dependencies. TABLE. V also demonstrates its advantage in anomaly detection using time-series PCC data.

TABLE VI: Advantages and Limitations of Model-based and Data-driven Cyber-attack Detection Methods.

	Model-based Methods	Data-driven Methods
Advantages	• Milder data requirement: Model-based methods usually prescribe the system model structures and some system parameters, leveraging established models and the given information about the system configuration that are relatively easier to obtain; have milder requirements for faulty data. When the system model is built, the system performance under cyber-attacks can be simulated, thereby avoiding the need for real-world faulty data that could be difficult to obtain.	• Minimal detection error since detailed model information is not required. The detection error is therefore not affected by the model uncertainty.
	• More mature and highly implementable: Model-based detection methods are relatively more mature, as they have been extensively applied for fault detection in the industry. The best practices and experiences developed for such methods could potentially be applied to cyber-attack detection applications and usually have less computational burden both in the detector preparation and in the real-time implementation stages.	• Ability to be trained offline and implemented online. Real-world data can be used to train a perfect model for a data-driven method, which reduces the risk for system operation.
Limitations	• Model accuracy. Model-based methods might not be able to provide accurate detection results since many real-world applications or phenomena lack an accurate model.	• Supervised learning methods require labeled information for the monitored data. Any error in the label information might lead to the failure of the trained model.
	• Unprecedented cyber-attack class. Model-based methods usually need to develop specified models for different cyber-attacks of interest. When a new class of cyber-attacks is encountered, model-based methods might provide inaccurate results. Data-driven methods can better handle such circumstances by using a generic detector, for example, which can discriminate between unprecedented cyber-attacks and normal operations.	• A large amount of historical data is required in the offline model training of the supervised learning method.

The advantages and limitations of model-based and data-driven methods are summarized in TABLE. VI.

C. Network and Firmware Security Detection and Mitigation Methodology

Network-based security techniques have been mostly proposed to address the vulnerabilities of PV system communication standards [42], [43], [98]–[106]. A cybersecurity roadmap for PV systems was released in 2017 [42]. The roadmap focused on communication networks and emphasized the role of all stakeholders in establishing a cyber-secure PV network. Sandia National Laboratories (SNL) investigated three advanced network-based defense mechanisms for DERs including network segmentation, encryption, and ”moving target” defense in a virtualized environment [43]. The National Renewable Energy Laboratory (NREL) has established several best practices to mitigate these network-related attacks. Examples include role-based user access control and strong key management, public key infrastructure (PKI), and certification management [99]. They also proposed the incorporation of an OT hardware module (i.e., Module-OT) into the PV inverter to strengthen its network security [100]. Software-defined networking (SDN) technology, where network operators flexibly manage the network, has been applied to a configurable network and access control with the goal of mitigating cyber-attacks, such as DoS attacks [101], [102]. Moreover, real-time network intrusion detection methods for PV inverters/systems have been widely studied to detect the forged in-transit-data, which includes: 1) Signature/rule-based network intrusion detection using tools such as Snort [103] and Suricata [107] (e.g., detecting irregular network packet format, reply, and message authentication); 2) Behavior-based machine learning [103], and signal processing methods (e.g., watermarking [104] and perturbation-based diagnostics [105]).

Software-related attacks can bypass the most advanced access control and security mechanisms [108]. Numerous cases of power grid devices’ firmware vulnerabilities have been reported [109]. To date, PV inverters’ real-time firmware security has not been explored as much as network-related security. A power router prototype using a dual-controller design has been proposed to improve uptime and firmware security for power grid devices [110]. The dual-controller design consists of one controller that provides pulse width modulation (PWM) signals to the PV inverter and another controller that examines the updated firmware by checking the generated PWM signals. A.P. Kuruvila et al. proposed a custom-built hardware performance counter (HPC) method to detect malicious firmware modifications in a PV inverter. The method consists of periodically measuring the order of various instruction types within the inverter firmware code and identifying an unwanted modification using machine learning-based classifiers [111]. A machine learning-based tool to automate security patches and vulnerability remediation for electric utilities has been proposed [112]. The machine learning engine automatically acquires applicable vulnerabilities from a central database that includes asset data and Common Vulnerability Scoring System (CVSS) attributes obtained from vendors, third-party services, or public databases. CKC-based defense methods can be used to detect sophisticated attackers early, before an actual impact occurs, and to neutralize sophisticated cyber-attacks by cutting a middle stage of the CKC model in both PIT and OT sides. D3FEND is a knowledge graph framework providing a countermeasure of MITRE's ATT&CK for ICS based CKC model [113]. The graph contains semantically rigorous types and relations that define both of the key concepts in the cybersecurity countermeasure domain.

Blockchain technology can provide a secure distributed system framework on currently available information and communication technology (ICT) applications utilizing the latest cryptography, PKI, consensus, smart contract, and access control mechanisms. Blockchain technology has been widely adopted in IoT applications and e-commerce systems for secure communications, data sharing, and software security [114], [115]. In the energy sector, blockchain technology has been mostly studied in secure or privacy-preserved energy trading [116], [117]. Recently, M. Mylrea et al. examined how blockchain technology can meet North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance requirements for software patching [118]. It is anticipated that the traceability, transparency, and accountability features of the blockchain technology could mitigate most of the challenges associated with patching critical IT and OT systems. Fig. 10 illustrates the overall concept of blockchain-based zero-trust ecosystem for a PV system (i.e., no network-related entity including sensitive data, devices, applications, and systems can be trusted) [45]. A private blockchain network can build a collaborative security ecosystem where multiparty (e.g., utility, operator, vendors, and security service provider) can seamlessly handle the user- or vendor-identified incidents through effective notification, coordination, disclosure, and validation mechanisms, while considering the privacy of the PV system using smart contract and multichannel blockchain. The consistent and continuous process of verifying identity, validating activity, and limiting access and privilege will increase the trustworthiness of the system security services to ensure the integrity and authenticity of critical assets, thus providing a viable way to manage the evolving cyber risks on PV systems. Security modules are attached/installed in the critical devices, such as the cloud, site data manager, and inverters. The security module mainly consists of a blockchain client program, IDS, static malware analysis, and firmware rollback/patch [119]. The blockchain client enables the submission of transactions, access ledgers, and public key infrastructure (PKI, as part of membership service), and such events can be controlled by smart contracts. Through the blockchain-based framework, the MITM attacks are detected by using the blockchain-based cooperative in-transit data verification process [45] and software/firmware update [119]. Fig. 11 shows the block diagram of the blockchain platform for an in-transit control command/file integrity validation scenario where the data are considered a critical asset; therefore, the authentication, integrity, and authorization of the critical in-transit data are kept verified, and the results are stored in the ledger as security logs. PV system vendors, an operator, utility, and security modules will be the clients that are authorized persons/devices providing data as a form of transactions to the blockchain network and can access/share the data stored in their blockchain ledgers. Uploading and accessing data in the ledgers are mutually agreed upon and programmed by smart contracts. Only authorized parties using the blockchain client program can create transactions that include hash values of control commands/files, and the blockchain network considers the control command or file update as an authorized event. Therefore, the blockchain network can provide increased visibility into the methods, applications, and services to easily ensure the integrity and authenticity of the control command/file assets. After they provide the hash values to the blockchain ledger, the smart contract is running the integrity check without trusting the existing security perimeters, such as the TLS and firewall whitelist. In addition to the file integrity check using blockchain, software/firmware update process includes static malware analysis (i.e., the file will be analyzed without open/run the file). In [119], an open-source software, PeStudio Ver. 9.09 is used to reverse the code engineering of the received files first in a Windows virtual machine. This tool provides cryptographic hash verification, original file information, signature, blacklists, and the level of risk information as clues of known malware types. It enables access to VirusTotal, an online suspicious file/URL scan website cooperating 69 antivirus engines; thus, a python code is developed and implemented in Raspberry Pi OS (Debian) in a virtual machine to perform similar static malware analysis, allowing communications with the blockchain server.

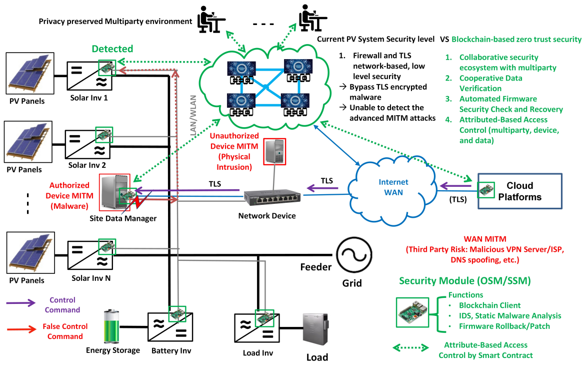

Privacy preserved Multiparty environment
- - -
Detected
PV Panels
Solar Inv 1
PV Panels
Solar Inv 2
LAN/WLAN
Authorized Device MITM (Malware)
Site Data Manager
Unauthorized Device MITM (Physical Intrusion)
TLS
Network Device
TLS
Internet WAN
(TLS)
Cloud Platforms
PV Panels
Solar Inv N
Feeder
Grid
Control Command
False Control Command
Energy Storage
Battery Inv
Load Inv
Load
Current PV System Security level VS Blockchain-based zero trust security
1. Firewall and TLS network-based, low level security
→ Bypass TLS encrypted malware
→ Unable to detect the advanced MITM attacks
1. Collaborative security ecosystem with multiparty
2. Cooperative Data Verification
3. Automated Firmware Security Check and Recovery
4. Attributed-Based Access Control (multiparty, device, and data)
WAN MITM
(Third Party Risk: Malicious VPN Server/ISP, DNS spoofing, etc.)
Security Module (OSM/SSM)
Functions
• Blockchain Client
• IDS, Static Malware Analysis
• Firmware Rollback/Patch
Attribute-Based Access Control by Smart Contract

Fig. 10: A concept of block-based zero-trust security for a PV system.

T. Kim et al. explored the cyber-physical security of battery management systems (BMSs) and the adoption of blockchain technology with IoT devices as defense strategies for security

TABLE VII: Comparison of State-of-art Strategies and Blockchain Security Adopted/To Be Adopted To PV Farm.

Security Category	State-of-the-Art Strategy	Blockchain-based Strategy
Network Security	• TLS, VPN, PKI	• Each device has its own ID and asymmetric key, resulting in eliminating complicated key management and distribution (membership service)
	• Network segmentation and moving target defense	• Smart contract-based access control and MITM attack detection
	• SDN	
Software/Firmware Security	• Design a secure compiler with a secure coding rule checker and a static weakness analyzer	• A smart contract allows to store the original hash of the firmware in the ledger to validate the firmware and automatically patch if corrupted
	• Code signing	• Static malware analysis
	• Automated detection for software vulnerabilities and automated patch generation	• Patch management
Data Storage Security	• Data storage will be locked and the data can be encrypted (e.g., hashing technique and MD5 encryption)	• Data integrity and privacy can be guaranteed through the distributed blockchain ledger since the blocks are linked and encrypted
On-board Interface Security	• Enforce recommendations from OWASP: 1) remove unnecessary physical interfaces (e.g., USB ports); 2) disable testing/debugging tools; and 3) implement TPM	• On-board network security might be guaranteed if a lightweight blockchain can be implemented at the on-board level
	• Detection methods for signal injection attacks	• Physically unclonable function (PUF) verified by blockchain
Hardware Security	• Functional safety checking of ICs	• Component-level authorization and supply chain management can act as a good defense strategy against insecure hardware replacements/insertions since the transactions on the ledger are immutable
	• Diagnostics for detecting damaged hardware components	
	• Asset-based structural checking tool for detecting abnormal electrical signal patterns	

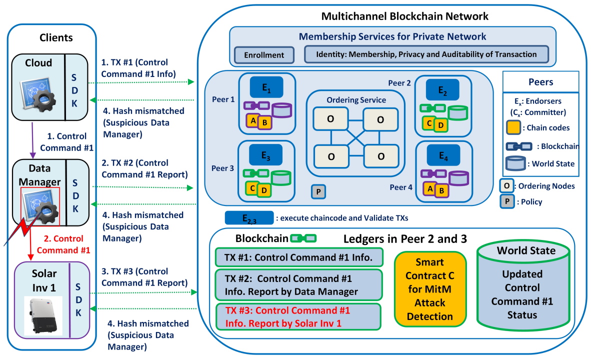

Clients
Cloud
SDK
Data Manager
SDK
Solar Inv 1
SDK
1. Control Command #1
2. Control Command #1
1. TX #1 (Control Command #1 Info)
4. Hash mismatched (Suspicious Data Manager)
2. TX #2 (Control Command #1 Report)
4. Hash mismatched (Suspicious Data Manager)
3. TX #3 (Control Command #1 Report)
4. Hash mismatched (Suspicious Data Manager)
Multichannel Blockchain Network
Membership Services for Private Network
Enrollment
Identity: Membership, Privacy and Auditability of Transaction
Peer 1
Peer 2
Peer 3
Peer 4
E_1
E_2
E_3
E_4
A B
C D
Ordering Service
O
P
Peers
E_x: Endorsers (C_x: Committer)
: Chain codes
: Blockchain
: World State
O : Ordering Nodes
P : Policy
$E_{2,3}$: execute chaincode and Validate TXs
Blockchain
Ledgers in Peer 2 and 3
TX #1: Control Command #1 Info.
TX #2: Control Command #1 Info. Report by Data Manager
TX #3: Control Command #1 Info. Report by Solar Inv 1
Smart Contract C for MitM Attack Detection
World State
Updated Control Command #1 Status

Fig. 11: Cooperative in-transit data (e.g., files for firmware update and contract command validation using blockchain).

sensitive layers of battery management systems, including network, software/firmware, data storage, on-board interface, and hardware layers [120]. Table VII illustrates a comparison of the state-of-the-art (SOA) defense strategies and adopting emerging blockchain-based technologies for a PV system based on [120]. Interested readers are referred to [120] for more details.

V. Designing Next-Generation Cyber-Secure Power Electronics Systems

Power electronics systems are increasingly using advanced controls to operate in a secure way and protect the interfaced assets such as PV systems from abnormal grid events as well as cyber-attacks. To achieve this goal, a strong interaction and interdependence among hardware (e.g., power converters), firmware (e.g., control and communication), generation assets (e.g., PV solar, wind turbine) and the electric power grid is required [3], [121]. In particular PV inverters can be vulnerable to cyber- attacks and particular attention should be paid to making their controls robust and reliable.

Communication-based protection schemes against cyber-attacks will depend on a variety of factors such as the system architecture, its control, and the level of reliability required [122]. Based on a smart integrated system, B. Kang et al. describe a PV system where an attack through its communication layer caused significant physical damage on the

PV systems by forcing the inverter off the maximum planned aggregated I-V curve power point [123]. Other related attack scenarios are initiated by communicating false information to mislead system operators, hence leading to system instability caused by the operators themselves. A.Y. Fard et al. analyzed the unstable operation of high penetration PV grids due to abnormal operations [124]. The proposed cybersecurity analytics method shows that active-reactive power (PQ) set-point manipulation at the secondary control layer of PV inverters can cause grid voltage instability. To mitigate this risk an additional protection layer to check the validity of the incoming PQ setpoint is added to the primary protection layer.

Communication protocols and their encryption play an important role in securing interconnected PV systems against cyber-attacks. These communication-based attacks can happen without the central system operator's knowledge since it can be easily mistaken for and confounded with PV assets intermittent behavior. Many of the industry communication protocols do not have adequate encryption to protect against cyber-attacks. In systems with connected distributed generation sources which are highly dependent on communication systems and smart meters, an intruder might have access to several communication nodes [125]. A single cybersecurity layer will not be sufficient to protect against these attacks. To achieve a higher level of reliability, the communication layer may require a redundant protection system. The ease of propagation of cyber-attacks in a power system depends on the degree of decentralization of the distributed energy resources such as PV solar [126]. With the advent of decentralizing communication and the IoT, patterns that lead to cyber-attacks can be recognized and detected in a cooperative and timely manner, without depending on a failure prone central data collector. Ultimately, the use of control and detection algorithms in these communication systems should be modeled, quantified and considered when computing the system's overall reliability metrics [20].

To detect cyber-attacks, the system's actual response should be continuously compared to its normal operating condition state via appropriate modeling techniques. A cyber-attack is detected when a known system variable deviates from its normal value and no longer correlates to other variables within the system. Y. Isozaki et al. proposed a detection methodology of cyber-attacks on DERs with high PV penetration targeting voltage regulation and over-voltage protection at the point of interconnection to grid [19]. The detection algorithm works best and damages are limited when only a small number of PV panels are involved. Another class of attacks are stealthy attacks which are undetectable by common intrusion detection mechanisms. These attacks can cause severe harm to power electronics-based grid systems that exhibit low virtual inertia [127]. The low virtual inertia nature of power electronics-based systems when interconnected with traditional synchronous generator-based grid systems creates a new opportunity (attack surface) for the attacker to inflict more harm within a short amount of time [127], [128]. As a result of these attacks, these systems can easily and quickly become unstable before the intrusion is detected and acted upon. Traditional synchronous-based grid systems, however are more stable due to their high inertia.

K.G. Lore et al. argue that cyber-attacks on grid-tied PV systems with a central unit controller can either be strategic or random [85], however there is still a lack of well-established standards for attack detection. As there is not yet a standardized strategy, there are efforts on different fronts to develop intrusion detection techniques. In one such instance, Olowu et al. classifies these methodologies into signature-based, anomaly-based, and specification-based detections strategies [129]. Attack detection methodologies based on pattern recognition usually employ state vector estimations from observed measurements. This state estimation can be implemented using model-based or data-driven strategies as discussed in this work. The latter strategies correlate the expected response of the system output to the individual PV panels output, while the residual of this comparison is computed and compared to a given threshold. To face the challenge of detecting cyber-attacks on photovoltaic plants, signature-based machine-learning and deep-learning algorithms have been proposed [13], [97]. These algorithms have shown great accuracy in diagnosing cyber-attacks; however they have not been field-validated in an actual PV system. The signature of a cyber-attack can also be seen in the physical layer. Thus, Y. Isozaki et al. proposed hybrid data-based and physical-informed detection methods based on the observation of variables such as voltage and reactive power fluctuations during transient periods [130], [131]. These last two cited works show that observation and detection based on physical variables can be slow. The reason for the long-drawn-out detection response is that the standards allow for some flexibility in operating limits during the transient response of grid tied PV systems. Ozai et al., in turn, present an anomaly-based strategy [132] for smart grids. In this work, the authors argue that methodologies that work with state estimation face difficulties in recovering state vectors in sparse networks. To address this problem, the authors propose a statistical correlation-based machine learning mechanism for large-scale and distributed systems. The best accuracy in intrusion detection, however, is theoretically verified by specification-based techniques. These techniques specify the desirable behavior of a system through a security policy and with the help of smart meters. For this last methodology, solutions were implemented for applications in smart grids [133], [134]. As with other anomaly-based detection techniques, there is still no specification-based methodology that especially addresses the cybersecurity of photovoltaic plants, to the best of our knowledge.

Given the specificity of these attacks and that there are established detection methods, some recent studies proposed control-based solutions to mitigate their effect [15], [16], [135], [136]. These solutions control and impact the outcome through the converter power semiconductor switching devices. At the system level, resiliency to cyber-attacks requires a tight cyber-physical integration amongst all constituent sub-systems (e.g., converters) and the cyber layer (e.g., communication, detection algorithms, control) to thwart cyber-attacks.

The hybrid detection method leverages the flexible tools from the model-based and data-driven detection algorithms [137], [138]. From the model-based detection point of view, the motivation for hybrid cyber-attack detection method includes: 1)

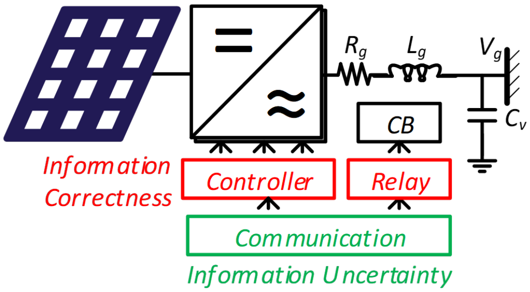


Fig. 12: Overview of cyber security issues in PV systems – information uncertainty and correctness may affect the control and protection layers simultaneously.

System model inaccuracies; and 2) Difficulty finding threshold for residuals. The latter can be a big issue for PV system cyber-attack detection. The threshold method is a simple criterion which is based on the value of the residuals. If the residual crosses the threshold value, the system is believed to be under attack. Given the variability and uncertainty in PV generation, the threshold needs to be designed not only to reflect the difference between the anomaly and normal conditions but also to take into consideration their differences under disturbed conditions. For this reason, the threshold can be difficult to find for certain applications. Thus, data-driven classification methods can be applied to replace the simple threshold-based method [139]. For example, CNN based classifiers can be developed to extract features beyond values of the residuals. These features could potentially yield rich information helpful for cyber-attack detection [140].

A. Challenges

Although the detection and mitigation approaches described above provide the technical foundations for dealing with cyber-attacks on PV systems, there remain several challenges to solve in order to secure them. These challenges mainly arise from vulnerabilities in the PV system controls and communication layer. Described below are four prominent examples of these challenges:

Wide Range of Time Scales (μs to min.): Since PV systems control dynamics operate at different timescales (microseconds to minutes), cybersecurity solutions need to operate from microseconds to minutes. An attack on the fastest control layer such as switching devices and gate drives requires fast cybersecurity solutions, while an attack on the slowest control layer such as the plant controller might be more manageable. Another challenge is discriminating between a cyber-attack and a fault. A thorough vulnerability assessment of PV system control loops against cyber-attacks is therefore key to its cyber-security.

Control Under Information Uncertainty: Figure 12 shows a PV system and its control, communication, and protection layers. Either a cyber intrusion or impaired communication traffic (e.g., latency, link failure, packet loss) can corrupt the transmitted data to the PV inverter causing information uncertainty. This uncertainty adversely affects the PV inverter control layer which in turns leads to real-time operation failures such as inability to respond to voltage and frequency ride-through, and Volt-Var Control. Furthermore, this information uncertainty will also affect the PV inverter control layer computation process (usually operating at a faster - μs - timescale). It will also impact circuit breaker protection relays as it will either delay or cancel relay trip decisions when grid faults occur. To address this challenge, communication network reliability and intrusion detection solutions must be implemented at the system and device level.

Scalability and Grid Transition: Scaling cyber-security solutions from device to system level poses an additional challenge. For PV systems, cyber-securing the PV inverter is important, but additional cyber-security measures need to be taken at the grid level. The latter will become more challenging as PV inverters are transitioning from grid-following to grid-forming. Grid-forming PV inverters will require complex and advanced controls to regulate the grid voltage and frequency. In a large PV farm there might be tens if not hundreds of these PV inverters, hence scaling cyber-security solutions from the inverter to the plant level is required.

Interoperability: As PV solar energy has become increasingly competitive, large (Hundreds of MegaWatts to few GigaWatts) plants are being deployed worldwide. These large plants include many PV panels (in the Millions) and PV inverters (in the Hundreds or Thousands if string inverters are used). Under these conditions interoperability amongst PV inverters is crucial to ensuring the plant cybersecurity. In addition to grid-following and forming, PV inverters perform many other functions such as fault-ride through, black-start, reactive power compensation, etc. To ensure optimal cyber-physical interaction amongst these PV inverters various syntactic compatibility reinforcements need to be monitored carefully as per the international standards for communication, which defines structural interoperability. Moreover, semantic interoperability is another challenge that rises when the structure and codification of data are non-uniform among all systems and sub-systems. Cybersecurity has therefore emerged as another metric when multiple power electronics converters need to be coordinated. Standardization of practices, policies for secure exchange of information is also critical critical for PV systems to securely perform their grid functions such as frequency regulation and demand response.

B. Future Directions

Cyber-physical security must keep pace with advances in control and computing techniques. The detection and mitigation methods for cyber-attacks have challenges as mentioned above. To bridge the gaps and meet these challenges, we propose, to expand the current research and work into the following new topics.

Multi-scale Controllability: To extend the current research to multi-scale controllability of grid-tied power electronic converters, a significant focus needs to be put on evaluating how cyber attackers impact large power systems. These attacks not only lead to shutdown and grid instability but also affect the grid

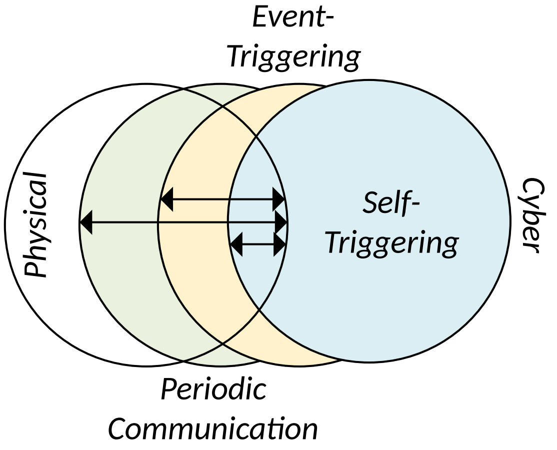


Fig. 13: Reduced cyber-physical interactions from periodic communication to self-triggering.

operation from an economic perspective. Resilience measures against cyber-attacks should be implemented at all levels and across time scales. Multi-scale controllability should enhance spacial temporal scalability across all the layers and events ranging from slow updates to cyber layers to faster disturbances in converters and the switching layers. This functionality will ultimately induce controllability over each function, such as MPPT, voltage regulation, switching losses reduction, and Electro Magnetic Interference (EMI) mitigation.

Event and Self-triggering Control: To simultaneously minimize both the cyber-physical interactions and provide resiliency against cyber-attacks, as shown in Figure 13, event and self-triggering control techniques are deployed. An event is defined as any cyber-physical disturbance to the system and is characterized by the measured values beyond a particular state-dependent threshold. Event-triggering control is an aperiodic concept that consists of only updating triggering signals when the system is in a quasi-stable mode. This reduces both the system computation and communication burden and only activates the communication layer during these events [141]–[143]. Self-triggering control uses a local entity to generate the triggering instants for each converter thereby reducing the need for communication between the converter and plant controllers. It can also be defined and tuned subject to the system noise. In addition to reducing computational and communication burdens, these triggering control techniques can also be used to schedule the exchange of information (such as PQ set-points) between PV systems and the grid as requested by the local Independent System Operator (ISO), such as NYISO, CAISO. As a result, any false data injected by a cyber attacker can be easily detected as it results in false command that does not fit the event-triggering criteria.

Artificial Intelligence and Machine Learning: Artificial Intelligence (AI) and Machine Learning (ML) are recent tools that are being deployed to make intelligent and data-driven device and system level control decisions based on the data generated by the actual system as well as its model. Specifically, in power systems with a high penetration of power electronics-based converters, accurate models are important and are validated by reinforced intelligence learning and abstraction AI/ML-based tools. These tools use a digital twin of the PV system to perform fault diagnostics and condition monitoring as well as expedite the resiliency of grid-tied PV systems against cyber-attacks using historical data. The tools' performance accuracy depends mainly on the volume and quality of the current and historical data, hence further research is required to develop sorting methods to screen and classify the data accordingly. For PV systems' cybersecurity purposes, it is essential to collect the system's response under various conditions such as grid faults, load shedding, contingencies, and data interruption from sensors and controllers.

Distributed Decision Making: Distributed decision-making is one of the most reliable means of information sharing in a multi-function power electronics system due to its communication infrastructure low cost, its scalability, and its resiliency against delays and link failures. Compared to a centralized information-sharing mechanism, distributed decision-making efficiently uses a common consensus point to reach a system level collective decision. This could be another PV systems attribute to ensure resiliency against cyber-attacks. A distributed sharing mechanism is more robust to attacks than a centralized mechanism since more points need to be compromised to destabilize the system versus a single central point. As a result, considerable system information is required by the cyber attacker to destabilize a distributed decision-making process system.

Hot-Patching and Online Security Performance: Hot-Patching is the ability to perform a firmware patch (to update, fix or improve) on a given device control unit without causing any downtime or any disruption to the system operation. Hot-Patching can reduce the cost and risk of system downtime during a firmware upgrade. Therefore, while the firmware update is being developed, tested, and patched, the entire system can continue running without interruptions. Generally, the firmware update is tested for vulnerabilities offline and once it passes the tests, the firmware is transmitted to the device and deployed in real time. When dealing with multiple devices' firmware updates, a time schedule for disconnecting, patching, and re-connecting the devices to the grid is established. When the firmware is ready to be patched, Hot-Patching allows for all of the devices to be simultaneously patched without interrupting the power flow of the PV system.

The architecture of a Hot-Patch capable device requires embedded parts that allow for the firmware patch to be performed while the rest of the controller is actively managing the grid-connected device. Having dedicated components in the controller that perform independent functions, such as firmware patching, allows for embedding security measures as part of the independent functions. When multiple vulnerabilities are discovered in different device controllers, they need to be immediately addressed and the corresponding firmware needs to be updated, which is time consuming. Fengli et al. demonstrated a patch scheduling methodology that prevents and denies opportunities for the attackers to exploit system vulnerabilities [144]. This scheduling methodology also takes into consideration the time-sensitivity of updating software vulnerabilities and the device downtime needed to patch the firmware. Hot-Patching and embedded security system concepts allow for an additional backup in the control layer when firmware vulnerabilities are being updated. If the vulnerabilities are not patched in a timely manner, they can be exploited by an attacker to send compromised commands to the system control layer. The embedded security hardware and firmware will evaluate these commands before they are transmitted to the system active controller. As an example, if the attacker sends a malicious firmware update that could harm the system, the embedded security hardware and firmware feature will screen these commands before they are implemented in the active controller.

Resilient Control Under Compromised Conditions: The electric power grid is a network system that is designed to serve a variety of consumers and stakeholders. Even when cybersecurity measures are implemented, the grid may still be vulnerable to cyber-attacks via a variety of attack surfaces. Attack-tolerant control algorithms to allow a power system to sustain its operation are critical to resilience against cyber-physical attacks. To maintain sustainable operation even when a small portion of the system is compromised, some solutions have been proposed in the literature. N. Gajanur et al. proposed blockchain-assisted inverter secondary control in which blockchain serves as a secure communication medium [145]. Though high-security methods with multiple security measures such as blockchain may incur additional latency, resulting from reinforced cybersecurity measures, the system can continue to operate under severe cyber-attacks. These attacks may compromise a portion of the primary communication and control system. M. Greidanus et al. proposed advanced controls to compensate for the impact of the security measures, e.g., increased latency [146].

In the legacy grid, a cyber-attack or a natural disaster will lead to outages at all distribution feeders, including feeders that are tied to DER assets such as PV. This is due to the mode of operation of grid-following PV inverters, which are unable to operate in an islanding mode. To operate and to form the voltage and frequency of an isolated, inverter-based DER distribution local grid, *grid-forming* inverter controls are used to independently black-start it when the main grid experiences a blackout [147], [148]. By allowing multiple PV inverters to collectively manage the local grid, without relying on high-fidelity communications, grid resilience can be achieved. To enhance the survivability of a power system against cyber-physical attacks, system operators should consider limiting the use of external network-based communications and instead rely on robust internal communication as much as possible. Although the use of internal communications might not be optimal, it does have the benefits of ensuring service continuity and facilitating the recovery process during and post cyber-attack events.

VI. Conclusion

This paper presented a comprehensive review and status of PV systems' cyber-physical security. This includes vulnerability analysis, impact assessment, attack detection and mitigation, and future research topics. Cyber-physical security was addressed from a hardware, firmware, communications, and network perspective. Impacts and security assessment preliminary results were described and presented. To address cyber threat detection and mitigation, model-based and data-driven methodologies are proposed. In addition, blockchain algorithms are also suggested as a way to counter cyber-attacks on the communication networks. Additional ideas include multi-scale system modeling, event-trigger control, artificial intelligence application, and hot patching. The ideas proposed have the potential to address the increasing challenges posed by cyber-attacks on renewable assets in general and on PV systems in particular.

References

[1] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber-physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges and future visions," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2020.

[2] 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*, 2019.

[3] S. K. Mazumder, A. Kulkarni, S. Sahoo, F. Blaabjerg, A. Mantooth, J. Balda, Y. Zhao, J. Ramos-Ruiz, P. 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*, 2021.

[4] J. C. Balda, A. Mantooth, R. Blum, and P. Tenti, "Cybersecurity and power electronics: Addressing the security vulnerabilities of the internet of things," *IEEE Power Electronics Magazine*, vol. 4, no. 4, pp. 37–43, Dec 2017.

[5] L. K. A. Terashmila, T. Iqbal, and G. Mann, "A comparison of low cost wireless communication methods for remote control of grid-tied converters," in *IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*. IEEE, 2017, pp. 1–4.

[6] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE transactions on Industrial informatics*, vol. 7, no. 4, pp. 529–539, 2011.

[7] H. Benkraouda, M. A. Chakkantakath, A. Keliris, and M. Maniatakos, "Snifu: Secure network interception for firmware updates in legacy plcs," in *2020 IEEE 38th VLSI Test Symposium (VTS)*, 2020, pp. 1–6.

[8] J. Zhang, J. Ye, L. Guo, F. Li, and W. Song, "Vulnerability assessments for power-electronics-based smart grids," in *IEEE Energy Conversion Congress and Exposition (ECCE)*, 2020, pp. 1702–1707.

[9] J. Zhang, Q. Li, J. Ye, and L. Guo, "Cyber-physical security framework for photovoltaic farms," in *2020 IEEE CyberPELS*, 2020, pp. 1–7.

[10] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Transactions on industrial informatics*, vol. 13, no. 5, pp. 2693–2703, 2017.

[11] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2018.

[12] F. Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, J. Ye, and W. Song, "Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2019.

[13] F. Li, Q. Li, J. Zhang, J. Kou, J. Ye, W. Song, and A. H. Mantooth, "Detection and diagnosis of data integrity attacks in solar farms based on multi-layer long short-term memory network," *IEEE Transactions on Power Electronics*, 2020.

[14] Y. Li, P. Zhang, L. Zhang, and B. Wang, "Active synchronous detection of deception attacks in microgrid control systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 1, pp. 373–375, 2017.

[15] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Resilient operation of heterogeneous sources in cooperative dc microgrids," *IEEE Transactions on Power Electronics*, vol. 35, no. 12, pp. 12 601–12 605, 2020.

[16] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, "Resilient networked AC microgrids under unbounded cyber attacks," *IEEE Transactions on Smart Grid*, 2020.

[17] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, S. Sargolzaei, and B. Carbunar, "Resilient design of networked control systems under time delay switch attacks, application in smart grid," *IEEE Access*, vol. 5, pp. 15 901–15 912, 2017.

[18] A. Barua and M. A. Al Faruque, "Hall spoofing: A non-invasive dos attack on grid-tied solar inverter," in *29th {USENIX} Security Symposium ({USENIX} Security 20)*, 2020, pp. 1273–1290.

[19] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, "Detection of cyber attacks against voltage control in distribution power grids with pvs," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1824–1835, 2015.

[20] P. Zhang, W. Li, S. Li, Y. Wang, and W. Xiao, "Reliability assessment of photovoltaic power systems: Review of current status and future perspectives," *Applied energy*, vol. 104, pp. 822–833, 2013.

[21] U. Jahn and W. Nasse, "Performance analysis and reliability of grid-connected pv systems in iea countries," in *3rd World Conference onPhotovoltaic Energy Conversion, 2003. Proceedings of*, vol. 3, 2003, pp. 2148–2151 Vol.3.

[22] A. Golnas, "Pv system reliability: An operator's perspective," in *2012 IEEE 38th Photovoltaic Specialists Conference (PVSC) PART 2*, 2012, pp. 1–6.

[23] D. S. Pillai, F. Blaabjerg, and N. Rajasekar, "A comparative evaluation of advanced fault detection approaches for pv systems," *IEEE Journal of Photovoltaics*, vol. 9, no. 2, pp. 513–527, 2019.

[24] T. Esram and P. L. Chapman, "Comparison of photovoltaic array maximum power point tracking techniques," *IEEE Transactions on energy conversion*, vol. 22, no. 2, pp. 439–449, 2007.

[25] I. Yahyaoui, *Advances in Renewable Energies and Power Technologies: Volume 1: Solar and Wind Energies*. Elsevier, 2018.

[26] M. Alam, K. Muttaqi, and D. Sutanto, "A novel approach for ramp-rate control of solar pv using energy storage to mitigate output fluctuations caused by cloud passing," *IEEE Transactions on Energy Conversion*, vol. 29, no. 2, pp. 507–518, 2014.

[27] P. Guerriero, L. Piegari, R. Rizzo, and S. Daliento, "Mismatch based diagnosis of pv fields relying on monitored string currents," *International Journal of Photoenergy*, vol. 2017, 2017.

[28] "How to protect your solar panels from thieves?" [Online]. Available: https://www.ledwatcher.com/how-to-protect-your-solar-panels-from-thieves/

[29] K. Galbraith, "Solar panels are vanishing, only to reappear on the internet." [Online]. Available: https://www.nytimes.com/2008/09/24/technology/24solar.html

[30] K. Misbrener, "Cyberattacks threaten smart inverters, but scientists have solutions." [Online]. Available: https://www.solarpowerworldonline.com/2019/04/cyberattacks-threaten-smart-inverters-but-scientists-have-solutions/

[31] S. Nichols, "Cigar 'smokes out' attacks on solar electrical power equipment." [Online]. Available: https://crd.lbl.gov/news-and-publications/news/2021/cigar-smokes-out-attacks-on-solar-electrical-power-equipment/

[32] M. Aminzade, "Confidentiality, integrity and availability–finding a balanced it framework," *Network Security*, vol. 2018, no. 5, pp. 9–11, 2018.

[33] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[34] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: a survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101–115, 2019.

[35] J. Zhang, L. Guo, and J. Ye, "Hardware-in-the-loop testbed for cyber-physicalsecurity of photovoltaic farms," in *2021 IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, 2021.

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

[37] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE transactions on control of network systems*, vol. 1, no. 4, pp. 370–379, 2014.

[38] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient merkle-tree-based authentication scheme for smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 655–663, 2013.

[39] C. Zhao, J. He, P. Cheng, and J. Chen, "Analysis of consensus-based distributed economic dispatch under stealthy attacks," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5107–5117, 2016.

[40] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, 2014.

[41] S. Harshbarger, M. Hosseinzadehtaher, B. Natarajan, E. Vasserman, M. Shadmand, and G. Amariucai, "(a little) ignorance is bliss: The effect of imperfect model information on stealthy attacks in power grids," in *2020 IEEE Kansas Power and Energy Conference (KPEC)*, 2020, pp. 1–6.

[42] J. Johnson, "Roadmap for photovoltaic cyber security," *Sandia National Laboratories*, 2017.

[43] J. Johnson, I. Onunkwo, P. Cordeiro, B. J. Wright, N. Jacobs, and C. Lai, "Assessing der network cybersecurity defences in a power-communication co-simulation environment," *IET Cyber-Physical Systems: Theory Applications*, vol. 5, no. 3, pp. 274–282, 2020.

[44] "Alert (aa20-352a)," [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-352a, Tech. Rep., 2017.

[45] J. Choi, B. Ahn, S. Ahmad, D. Narayanasamy, Zeng, J, and T. Kim, "A real-time hardware-in-the-loop (hil) cybersecurity testbed for power electronics devices and systems in cyber-physical system environments," in *2021 IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, 2021.

[46] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Multilayer resilience paradigm against cyber attacks in dc microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 3, pp. 2522–2532, 2020.

[47] A. Khan, M. Hosseinzadehtaher, M. B. Shadmand, D. Saleem, and H. Abu-Rub, "Intrusion detection for cybersecurity of power electronics dominated grids: Inverters pq set-points manipulation," in *2020 IEEE CyberPELS*, 2020, pp. 1–8.

[48] H. Lee, K. Kim, J.-H. Park, G. Bere, J. J. Ochoa, and T. Kim, "Convolutional neural network-based false battery data detection and classification for battery energy storage systems," *IEEE Transactions on Energy Conversion*, 2021.

[49] J. Choi, B. Ahn, G. Bere, S. Ahmad, A. Mantooth, and T. Kim, "Blockchain-based man-in-the-middle (mitm) attack detection for photovoltaic systems," in *2021 IEEE Design Methodologies for Power Electronics*, 2021.

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

[51] G. Bere, B. Ahn, J. Ochoa, J, T. Kim, A. Hadi, A, and J. Choi, "Blockchain-based firmware security check and recovery for smart inverters," in *2021 IEEE Applied Power Electronics Conference and Exposition (APEC)*, 2021.

[52] L. Huang and Q. Zhu, "A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems," *Computers & Security*, vol. 89, p. 101660, 2020.

[53] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power system reliability evaluation considering load redistribution attacks," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 889–901, 2016.

[54] K. Monnappa, *Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware*. Packt Publishing Ltd, 2018.

[55] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29 775–29 818, 2021.

[56] "Highly evasive attacker leverages solarwinds supply chain to compromise multiple global victims with sunburst backdoor," [Online]. Available: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html, Tech. Rep.

[57] R. S. de Carvalho and D. Saleem, "Recommended functionalities for improving cybersecurity of distributed energy resources," in *2019 Resilience Week (RWS)*, vol. 1, 2019, pp. 226–231.

[58] Att&ck for industrial control systems. [Online]. Available: collaborate.mitre.org/attackics/index.php/Main_Page

[59] G. Jakobson, "Mission cyber security situation assessment using impact dependency graphs," in *14th International Conference on Information Fusion*, 2011, pp. 1–8.

[60] A. Giani and R. Bent, "Addressing smart grid cyber security," in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, 2013, pp. 1–4.

[61] S. Sahoo and J. C.-H. Peng, “A localized event-driven resilient mechanism for cooperative microgrid against data integrity attacks,” *IEEE Transactions on Cybernetics*, 2020.

[62] X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, and X. Liu, “Microgrid risk analysis considering the impact of cyber attacks on solar pv and ess control systems,” *IEEE transactions on smart grid*, vol. 8, no. 3, pp. 1330–1339, 2016.

[63] “Solar accounts for 40% of u.s. electric generating capacity additions in 2019,” [Online]. Available: https://www.seia.org/news/solar-accounts-40-us-electric-generating-capacity-additions-2019-adds-133-gw, Tech. Rep., 2019.

[64] B. Sobczak, “’Cyber event’ disrupted U.S. grid networks,” https://www.eenews.net/stories/1060242741/, 2021, [Online; accessed 9-March-2021].

[65] A. Teymouri, A. Mehrizi-Sani, and C.-C. Liu, “Cyber security risk assessment of solar pv units with reactive power capability,” in *IECON 2018 Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 2872–2877.

[66] C. Yi, D. Julia, L. Jason, D. Scott, S. Anoop, and O. Xinming. Metrics of security. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=917850

[67] S. Sahoo, J. C.-H. Peng, A. Devakumar, S. Mishra, and T. Dragičević, “On detection of false data in cooperative dc microgrids—a discordant element approach,” *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 6562–6571, 2019.

[68] S. Tan, J. M. Guerrero, P. Xie, R. Han, and J. C. Vasquez, “Brief survey on attack detection methods for cyber-physical systems,” *IEEE Systems Journal*, vol. 14, no. 4, pp. 5329–5339, 2020.

[69] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[70] E. Handschin, F. C. Schweppe, J. Kohlas, and A. Fiechter, “Bad data analysis for power system state estimation,” *IEEE Transactions on Power Apparatus and Systems*, vol. 94, no. 2, pp. 329–337, 1975.

[71] K. Clements and P. Davis, “Multiple bad data detectability and identifiability: a geometric approach,” *IEEE Transactions on Power Delivery*, vol. 1, no. 3, pp. 355–360, 1986.

[72] M. Cheniae, L. Mili, and P. Rousseeuw, “Identification of multiple interacting bad data via power system decomposition,” *IEEE Transactions on Power Systems*, vol. 11, no. 3, pp. 1555–1563, 1996.

[73] K. Clements and P. Davis, “Detection and identification of topology errors in electric power systems,” *IEEE Transactions on Power systems*, vol. 3, no. 4, pp. 1748–1753, 1988.

[74] Y. Zhang, J. Wang, and J. Liu, “Attack identification and correction for pmu gps spoofing in unbalanced distribution systems,” *IEEE transactions on smart grid*, vol. 11, no. 1, pp. 762–773, 2019.

[75] J. Liu, R. Singh, and B. C. Pal, “Distribution system state estimation with high penetration of demand response enabled loads,” *IEEE Transactions on Power Systems*, pp. 1–1, 2021.

[76] F. Pasqualetti, F. Dörfler, and F. Bullo, “Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design,” in *2011 50th IEEE Conference on Decision and Control and European Control Conference*. IEEE, 2011, pp. 2195–2201.

[77] A. Meng, H. Wang, S. Aziz, J. Peng, and H. Jiang, “Kalman filtering based interval state estimation for attack detection,” *Energy Procedia*, vol. 158, pp. 6589–6594, 2019.

[78] J. Chen and R. J. Patton, *Robust model-based fault diagnosis for dynamic systems*. Springer Science & Business Media, 2012, vol. 3.

[79] E. Frisk and M. Nyberg, “A minimal polynomial basis solution to residual generation for fault diagnosis in linear systems,” *Automatica*, vol. 37, no. 9, pp. 1417–1424, 2001.

[80] J. Zhang, H. Yao, and G. Rizzoni, “Fault diagnosis for electric drive systems of electrified vehicles based on structural analysis,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1027–1039, 2017.

[81] X. Ren, J. Yan, and Y. Mo, “Binary hypothesis testing with byzantine sensors: Fundamental tradeoff between security and efficiency,” *IEEE Transactions on Signal Processing*, vol. 66, no. 6, pp. 1454–1468, 2018.

[82] B. Kailkhura, Y. S. Han, S. Brahma, and P. K. Varshney, “Asymptotic analysis of distributed bayesian detection with byzantine data,” *IEEE Signal Processing Letters*, vol. 22, no. 5, pp. 608–612, 2014.

[83] H. Wang, J. Ruan, G. Wang, B. Zhou, Y. Liu, X. Fu, and J. Peng, “Deep learning-based interval state estimation of ac smart grids against sparse cyber attacks,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4766–4778, 2018.

[84] F. Wei, Z. Wan, and H. He, “Cyber-attack recovery strategy for smart grid based on deep reinforcement learning,” *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2476–2486, 2019.

[85] K. G. Lore, D. M. Shila, and L. Ren, “Detecting data integrity attacks on correlated solar farms using multi-layer data driven algorithm,” in *2018 IEEE Conference on Communications and Network Security (CNS)*, 2018, pp. 1–9.

[86] H. Karimipour, A. Dehghantanha, R. M. Parizi, K.-K. R. Choo, and H. Leung, “A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids,” *IEEE Access*, vol. 7, pp. 80 778–80 788, 2019.

[87] F. Li, Y. Shi, A. Shinde, J. Ye, and W. Z. Song, “Enhanced cyber-physical security in internet of things through energy auditing,” *IEEE Internet of Things Journal*, vol. 6, pp. 5224–5231, 2019.

[88] P. Filonov, A. Lavrentyev, and A. Vorontsov, “Multivariate industrial time series with cyber-attack simulation: Fault detection using an lstm-based predictive data model,” *arXiv preprint arXiv:1612.06676*, 2016.

[89] Z.-H. Yu and W.-L. Chin, “Blind false data injection attack using pca approximation method in smart grid,” *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1219–1226, 2015.

[90] J. Giraldo, A. Cárdenas, and N. Quijano, “Integrity attacks on real-time pricing in smart grids: impact and countermeasures,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2249–2257, 2016.

[91] F. Li, R. Xie, Z. Wang, L. Guo, J. Ye, P. Ma, and W. Song, “Online distributed iot security monitoring with multidimensional streaming big data,” *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4387–4394, 2019.

[92] D. Wilson, Y. Tang, J. Yan, and Z. Lu, “Deep learning-aided cyber-attack detection in power transmission systems,” in *2018 IEEE Power Energy Society General Meeting (PESGM)*, 2018, pp. 1–5.

[93] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, “Online cyber-attack detection in smart grid: A reinforcement learning approach,” *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5174–5185, 2018.

[94] J. Sakhnini, H. Karimipour, and A. Dehghantanha, “Smart grid cyber attacks detection using supervised learning and heuristic feature selection,” in *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*, 2019, pp. 108–112.

[95] 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 Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.

[96] X. Niu, J. Li, J. Sun, and K. Tomsovic, “Dynamic detection of false data injection attack in smart grid using deep learning,” in *2019 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2019, pp. 1–6.

[97] Q. Li, F. Li, J. Zhang, J. Ye, W. Song, and A. Mantooth, “Data-driven cyberattack detection for photovoltaic (pv) systems through analyzing micro-pmu data,” in *2020 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2020, pp. 431–436.

[98] C. Lai, N. Jacobs, S. Hossain-McKenzie, C. Carter, P. Cordeiro, I. Onunkwo, and J. Johnson, “Cyber security primer for der vendors, aggregators, and grid operators,” *Tech. Rep.*, vol. 12, 2017.

[99] 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 Systems Journal*, vol. 14, no. 1, pp. 17–27, 2019.

[100] W. Hupp, A. Hasandka, R. S. de Carvalho, and D. Saleem, “Module-ot: A hardware security module for operational technology,” in *2020 IEEE Texas Power and Energy Conference (TPEC)*, 2020, pp. 1–6.

[101] Y. Li, Y. Qin, P. Zhang, and A. Herzberg, “Sdn-enabled cyber-physical security in networked microgrids,” *IEEE Transactions on Sustainable Energy*, vol. 10, no. 3, pp. 1613–1622, 2018.

[102] P. Danzi, M. Angjelichinoski, Č. Stefanović, T. Dragičević, and P. Popovski, “Software-defined microgrid control for resilience against denial-of-service attacks,” *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5258–5268, 2018.

[103] C. B. Jones, A. R. Chavez, R. Darbali-Zamora, and S. Hossain-McKenzie, “Implementation of intrusion detection methods for distributed photovoltaic inverters at the grid-edge,” in *2020 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2020, pp. 1–5.

[104] J. Ramos-Ruiz, J. Kim, W.-H. Ko, T. Huang, P. Enjeti, P. R. Kumar, and L. Xie, “An active detection scheme for cyber attacks on grid-tied pv systems,” in *2020 IEEE CyberPELS (CyberPELS)*, 2020, pp. 1–6.

[105] K. Jhala, P. Pradhan, and B. Natarajan, “Perturbation-based diagnosis of false data injection attack using distributed energy resources,” *IEEE Transactions on Smart Grid*, 2020.

[106] A. A. Hadi, G. Bere, T. Kim, J. J. Ochoa, J. Zeng, and G.-S. Seo, "Secure and cost-effective micro phasor measurement unit (pmu)-like metering for behind-the-meter (btm) solar systems using blockchain-assisted smart inverters," in *2020 IEEE Applied Power Electronics Conference and Exposition (APEC)*, 2020, pp. 2369–2375.

[107] "Suricata," [Online]. Available: https://suricata.io/, Tech. Rep.

[108] C. Konstantinou and M. Maniatakos, "Impact of firmware modification attacks on power systems field devices," in *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2015, pp. 283–288.

[109] F. Zhang and Q. Li, "Security vulnerability and patch management in electric utilities: A data-driven analysis," in *Proceedings of the First Workshop on Radical and Experiential Security*, 2018, pp. 65–68.

[110] S. Moquin, S. Kim, N. Blair, C. Farnell, J. Di, and H. A. Mantooth, "Enhanced uptime and firmware cybersecurity for grid-connected power electronics," in *2019 IEEE CyberPELS (CyberPELS)*. IEEE, 2019, pp. 1–6.

[111] A. P. Kuruvila, I. Zografopoulos, K. Basu, and C. Konstantinou, "Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids," *arXiv preprint arXiv:2009.07691*, 2020.

[112] Q. Li, F. Zhang, and P. Huff, "Automated security patch and vulnerability remediation tool for electric utilities," Apr. 4 2019, uS Patent App. 16/150,042.

[113] "D3fend matrix," [Online]. Available: https://d3fend.mitre.org/, Tech. Rep.

[114] E. N. Witanto, Y. E. Oktian, S.-G. Lee, and J.-H. Lee, "A blockchain-based ocf firmware update for iot devices," *Applied Sciences*, vol. 10, no. 19, p. 6744, 2020.

[115] S. S. Seshadri, D. Rodriguez, M. Subedi, K.-K. R. Choo, S. Ahmed, Q. Chen, and J. Lee, "Iotcop: A blockchain-based monitoring framework for detection and isolation of malicious devices in internet-of-things systems," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3346–3359, 2020.

[116] "It's like the early days of the internet, blockchain-based microgrid tests p2p energy trading in brooklyn," [Online]. Available:http://microgridmedia.com/its-like-the-early-days-of-the-internet-blockchain-based-brooklyn-microgrid-tests-p2p-energy-trading/, Tech. Rep.

[117] T. Gaybullaev, H.-Y. Kwon, T. Kim, and M.-K. Lee, "Efficient and privacy-preserving energy trading on blockchain using dual binary encoding for inner product encryption," *Sensors*, vol. 21, no. 6, p. 2024, 2021.

[118] M. Mylrea and S. N. G. Gourisetti, "Blockchain for supply chain cybersecurity, optimization and compliance," in *2018 Resilience Week (RWS)*, 2018, pp. 70–76.

[119] T. Kim, J. Ochoa, T. Faika, A. Mantooth, J. Di, Q. Li, and Y. Lee, "An overview of cyber-physical security of battery management systems and adoption of blockchain technology," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–1, 2020.

[120] B. Ahn, S. Bere, S. Ahmad, J. Choi, and T. Kim, "Blockchain-enabled security module for transforming conventional inverters toward firmware security-enhanced smart inverters," in *2021 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2021.

[121] S. K. Mazumder, *Wireless networking based control*. Springer, 2011.

[122] A. A. Memon and K. Kauhaniemi, "A critical review of ac microgrid protection issues and available solutions," *Electric Power Systems Research*, vol. 129, pp. 23–31, 2015.

[123] B. Kang, P. Maynard, K. McLaughlin, S. Sezer, F. Andrén, C. Seitl, F. Kupzog, and T. Strasser, "Investigating cyber-physical attacks against iec 61850 photovoltaic inverter installations," in *2015 IEEE Conference on Emerging Technologies Factory Automation (ETFA)*, 2015, pp. 1–8.

[124] A. Khan, M. Hosseinzadehtaher, M. Shadmand, and S. Mazumder, "Cybersecurity analytics for virtual power plants," in *2021 IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, 2021.

[125] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45–56, 2018.

[126] H. Gunduz and D. Jayaweera, "Reliability assessment of a power system with cyber-physical interactive operation of photovoltaic systems," *International Journal of Electrical Power & Energy Systems*, vol. 101, pp. 371–384, 2018.

[127] A. Khan, M. Hosseinzadehtaher, M. B. Shadmand, S. Bayhan, and H. Abu-Rub, "On the stability of the power electronics-dominated grid: A new energy paradigm," *IEEE Industrial Electronics Magazine*, vol. 14, no. 4, pp. 65–78, 2020.

[128] O. H. Abu-Rub, A. Y. Fard, M. F. Umar, M. Hosseinzadehtaher, and M. B. Shadmands, "Towards intelligent power electronics-dominated grid via machine learning techniques," *IEEE Power Electronics Magazine*, vol. 8, no. 1, pp. 28–38, 2021.

[129] T. O. Olowu, S. Dharmasena, A. Hernandez, and A. Sarwat, "Impact analysis of cyber attacks on smart grid: A review and case study," in *New Research Directions in Solar Energy Technologies*, H. Tyagi, P. R. Chakraborty, S. Powar, and A. K. Agarwal, Eds. Singapore: Springer Singapore, 2021, pp. 31–51. [Online]. Available: https://doi.org/10.1007/978-981-16-0594-9_3

[130] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, "Detection of cyber attacks against voltage control in distribution power grids with pvs," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1824–1835, 2016.

[131] M. Greidanus, S. Mazumder, and N. Gajanur, "Identification of a delay attack in the secondary control of grid-tied inverter systems," in *IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, 2021.

[132] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 8, pp. 1773–1786, 2016.

[133] R. Mitchell and I.-R. Chen, "Behavior-rule based intrusion detection systems for safety critical smart grid applications," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1254–1263, 2013.

[134] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study," *IEEE Systems Journal*, vol. 9, no. 1, pp. 31–44, 2015.

[135] A. Y. Fard, M. B. Shadmand, and S. K. Mazumder, "Holistic multi-timescale attack resilient control framework for power electronics dominated grid," in *2020 Resilience Week (RWS)*, 2020, pp. 167–173.

[136] A.Y.Fard, M. Hosseinzadehtaher, M. Shadmand, and S. Mazumder, "Cyberattack resilient control for power electronics dominated grid with minimal communication," in *2021 IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, 2021.

[137] J.-A. Jiang, C.-L. Chuang, Y.-C. Wang, C.-H. Hung, J.-Y. Wang, C.-H. Lee, and Y.-T. Hsiao, "A hybrid framework for fault detection, classification, and location—part i: Concept, structure, and methodology," *IEEE Transactions on Power Delivery*, vol. 26, no. 3, pp. 1988–1998, 2011.

[138] M. Elnour, N. Meskin, and K. M. Khan, "Hybrid attack detection framework for industrial control systems using 1d-convolutional neural network and isolation forest," in *2020 IEEE Conference on Control Technology and Applications (CCTA)*, 2020, pp. 877–884.

[139] N. Markovic, T. Stoetzel, V. Staudt, and D. Kolossa, "Hybrid fault detection in power systems," in *2019 IEEE International Electric Machines Drives Conference (IEMDC)*, 2019, pp. 911–915.

[140] W. You, C. Shen, X. Guo, X. Jiang, J. Shi, and Z. Zhu, "A hybrid technique based on convolutional neural network and support vector regression for intelligent diagnosis of rotating machinery," *Advances in Mechanical Engineering*, vol. 9, no. 6, p. 1687814017704146, 2017.

[141] M. Tahir and S. K. Mazumder, "Event-and priority-driven coordination in next-generation grid," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 4, no. 4, pp. 1186–1194, 2016.

[142] W. Heemels, K. Johansson, and P. Tabuada, "An introduction to event-triggered and self-triggered control," in *2012 IEEE 51st IEEE Conference on Decision and Control (CDC)*, 2012, pp. 3270–3285.

[143] M. Tahir and S. K. Mazumder, "Self-triggered communication enabled control of distributed generation in microgrids," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 2, pp. 441–449, 2015.

[144] F. Zhang and Q. Li, "Dynamic risk-aware patch scheduling," in *2020 IEEE Conference on Communications and Network Security (CNS)*, 2020, pp. 1–9.

[145] N. Gajanur, M. Greidanus, G.-S. Seo, S. Mazumder, and M. Abbaszada, "Impact of blockchain delay on grid-tied solar inverter performance," in *IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, 2021.

[146] M. Greidanus, S. Sahoo, S. Mazumder, and F. Blaabjerg, "Novel control solutions to delay mitigation in grid connected and standalone inverters," in *IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, 2021.

[147] Y. Lin, J. H. Eto, B. B. Johnson, J. D. Flicker, R. H. Lasseter, H. N. Villegas Pico, G.-S. Seo, B. J. Pierre, and A. Ellis, "Research roadmap on grid-forming inverters," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2020.

[148] G.-S. Seo, M. Colombino, I. Subotic, B. Johnson, D. Groß, and F. Dörfler, "Dispatchable virtual oscillator control for decentralized inverter-dominated power systems: Analysis and experiments," in *2019 IEEE Applied Power Electronics Conference and Exposition (APEC)*, 2019, pp. 561–566.

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

She is currently an Assistant Professor of electrical engineering and the Director of the Intelligent Power Electronics and Electric Machines Laboratory, University of Georgia, Athens, GA, USA. Her current research interests include power electronics, electric machines, energy management systems, smart grids, electrified transportation, and cyber-physical systems. Dr. Jin Ye is the General Chair of 2019 IEEE Transportation Electrification Conference and Expo (ITEC), and the Publication Chair and Women in Engineering Chair of 2019 IEEE Energy Conversion Congress and Expo (ECCE). She is an Associate Editor for IEEE Transactions on Power Electronics, IEEE Open Journal of Power Electronics, IEEE Transactions on Transportation Electrification, and IEEE Transactions on Vehicular Technology.

Annarita Giani is a Senior Complex System Scientist at GE Research. She works on projects related to cybersecurity, critical infrastructure protection, energy systems, supply chain, modeling and simulation for situational awareness, machine learning and optimization for large dynamic, complex problems and quantum computing for industrial applications. Annarita has presented at international conferences and published over 50 articles in international conferences and journals. Before joining GE, Dr. Giani spent four years at Los Alamos National Laboratory working on cybersecurity of the energy grid. She started this research during her postdoc at the University of California at Berkeley. She holds a Ph.D. in Computer Engineering from Thayer School of Engineering at Dartmouth College and a Master's in Mathematics from the University of Pisa, Italy.

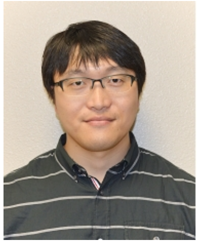
Ahmed Elasser (S'92, M'96, SM'12) was born in Demnate, Morocco in 1963. He received his Engineering Degree (Ingénieur D'Etat) from Ecole Mohammadia D'Ingenieurs, Rabat, Morocco in 1985 in Electric Power and Power Electronics. He spent seven years in Morocco working for industry and academia as a maintenance and laboratory engineer. He joined Rensselaer Polytechnic Institute in Troy, NY on a Fulbright Scholarship in 1992 and completed his MS and PhD degrees in Electric Power and Power Electronics in 1993 and 1996 respectively.

He joined GE Global Research Center in 1995 as a summer intern and is currently a Principal Systems Engineer in the areas of Electric Power, Power Electronics, and Power Semiconductor Devices. He worked on Silicon Power Devices such as IGBTs and IGCTs, Solar Energy, Silicon Carbide, Gallium Nitride, Power Conversion Systems Modeling and Simulation, Circuit Breakers, Power Systems, Battery Energy Storage, and Innovation. He published over 40 papers and has 37 patents issued with several pending. He recently gave keynote addresses on the past, present, and future of Battery Energy Storage Systems for the PCIM 2020 Digital Days and on the history and challenges of Silicon Carbide power devices at the 2019 IWIPP conference. Dr. Elasser is a Senior Member of IEEE and is a regular reviewer for many IEEE journals and conferences in his areas of expertise. Dr. Ahmed Elasser is the recipient of numerous GE Awards for his contributions and innovations over his 26 years GE career.

Sudip K. Mazumder (S'97–M'01–SM'03–F'16) received his Ph.D. degree from Virginia Tech in 2001. He is a Professor in the Department of Electrical and Computer Engineering at the University of Illinois, Chicago. He also serves as the President of NextWatt LLC since 2008. He was an IEEE Power Electronics Society (PELS) Distinguished Lecturer and the Chair for IEEE PELS Technical Committee on sustainable energy systems. He is the Editor-at-Large of IEEE Transactions on Power Electronics. He is a Fellow of the Institute of Electrical and Electronics Engineers (IEEE) and a Fellow of the American Association for the Advancement of Science (AAAS).

Chris Farnell NCREPT Managing Director and Test Engineer. Dr. Farnell (IEEE S'11 – M'19 - SM'21) received his Ph.D. degree in electrical engineering from the University of Arkansas in 2020. His research interests include Embedded System Design, Wireless Networks, FPGAs, Cybersecurity, and Power Electronics. He is currently serving as the Managing Director and Test Engineer for the National Center for Reliable Electric Power Transmission (NCREPT) at the University of Arkansas. Chris remains active in K-12 outreach activities.

H. Alan Mantooth received the B.S.E.E. and M.S.E.E. degrees from the University of Arkansas in 1985 and 1986, and the Ph.D. degree from Georgia Tech in 1990. He then joined Analogy, a startup company in Oregon, where he focused on semiconductor device modeling and the research and development of modeling tools and techniques. In 1998, he joined the faculty of the Department of Electrical Engineering at the University of Arkansas, Fayetteville, where he currently holds the rank of Distinguished Professor. His research interests now include analog and mixed-signal IC design & CAD, semiconductor device modeling, power electronics, power electronics packaging, and cybersecurity. Dr. Mantooth helped establish the National Center for Reliable Electric Power Transmission (NCREPT) at the UA in 2005. Professor Mantooth serves as the Executive Director for NCREPT as well as two of its centers of excellence: the NSF Industry/University Cooperative Research Center on GRid-connected Advanced Power Electronic Systems (GRAPES) and the Cybersecurity Center on Secure, Evolvable Energy Delivery Systems (SEEDS) funded by the U.S. Department of Energy. In 2015, he also helped to establish the UA's first NSF Engineering Research Center entitled Power Optimization for Electro-Thermal Systems (POETS) that focuses on high power density systems for electrified transportation applications. Dr. Mantooth has co-founded three companies in design automation (Lynguent), IC design (Ozark Integrated Circuits), and cybersecurity (Bastazo) as well as advising a fourth in power electronics packaging (Arkansas Power Electronics International) to maturity and acquisition as a board member. Dr. Mantooth holds the 21st Century Research Leadership Chair in Engineering. He currently serves as Senior Past-President for the IEEE Power Electronics Society and Editor-in-Chief of the IEEE Open Journal of Power Electronics. Dr. Mantooth is a Fellow of IEEE, a member of Tau Beta Pi and Eta Kappa Nu, and registered professional engineer in Arkansas.



Taesic Kim (S'10-M'15) received the B.S. degree in Electronics Engineering from Changwon National University, Changwon, Korea in 2008 and the M.S. and Ph.D. degree in Electrical Engineering and Computer Engineering from the University of Nebraska–Lincoln, in 2012 and 2015, respectively.

In 2009, He was with the New and Renewable Energy Research Group of Korea Electrotechnology Research Institute, Korea. He was also with Mitsubishi Electric Research Laboratories, Cambridge, MA, USA in 2013. Currently, he is an associate professor in the Department of Electrical Engineering and Computer Science at the Texas A&M University–Kingsville. His research interests cover broad areas of cyber-physical power and energy systems including cyber-physical security, battery management systems, energy IoT, power electronics, and blockchain. He was a recipient of the 2018 Myron Zucker Student–Faculty Grant Award from IEEE Foundation, the best paper award in the 2017 IEEE International Conference on Electro Information Technology, and the first prize award in the 2013 IEEE Industry Application Society Graduate Student Thesis Contest.

Jianzhe Liu (S'13-M'18) received the B.E. degree in electrical engineering from Huazhong University of Science and Technology, China, in 2012, and the Ph.D. degree in electrical and computer engineering from The Ohio State University, US, in 2017. Dr. Liu was a visiting scholar at Aalborg University, Denmark, in 2017. He is currently an Energy Systems Scientist at Argonne National Laboratory. His research interests include robust control and optimization for electric power systems.

Bo Chen (M'17) received the Ph.D. degree in electrical engineering from Texas A&M University, College Station, USA, in 2017. He received the B.S. and M.S. degrees from North China Electric Power University in 2008 and 2011, respectively. In 2017, he worked as a postdoc researcher at the Argonne National Laboratory, IL, USA. Currently, he is an Energy Systems Scientist at the Energy Systems Division, Argonne National Laboratory, IL, USA. His research interests include modeling, control, and optimization of power systems, cybersecurity, and cyber-physical systems. Dr. Chen is the Associate Editor of IEEE Transactions on Smart Grid.

Gab-Su Seo (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the Seoul National University, Seoul, South Korea, in 2015.

From 2016 to 2017, he was a Research Associate with the Colorado Power Electronics Center, University of Colorado, Boulder, CO, USA. Since 2018, he has been with the Power Systems Engineering Center, National Renewable Energy Laboratory (NREL), Golden, CO, USA, where he is currently a Senior Electrical Engineer and leads research projects focused on power electronics and power systems applications for electric grids with high penetration of inverter-based resources. He has coauthored more than 60 IEEE journal and conference papers with one best paper award. He coauthored the Research Roadmap on Grid-Forming Inverters (NREL) in 2020. His current research interests include power electronics for renewable energy systems and microgrids and power systems engineering for grid modernization including grid-forming inverter control for low or zero inertia grids to improve grid resilience and stability. Dr. Seo is an IEEE Roadmap Working Group Chair of the International Technology Roadmap of Power Electronics for Distributed Energy Resources (ITRD)—WG3 Integration and Control of DER. He is an Associate Editor of the IEEE Transactions on Power Electronics, the IEEE Access, the IEEE Open Journal of Power Electronics, and the Journal of Power Electronics.

Wenzhan Song received B.S. and M.S. degrees from Nanjing University of Science and Technology, Nanjing, China, in 1997 and 1999, respectively, and the Ph.D. degree in Computer Science from Illinois Institute of Technology, Chicago, IL, USA, in 2005. He is currently the Chair Professor of electrical and computer engineering with University of Georgia, Athens, GA, USA. His current research interests include cyber-physical systems and their applications in energy, environment, food and health sectors. Dr. Song was the recipient of the NSF CAREER award in 2010.

Subham Sahoo (S'16-M'18) received the B.Tech. & Ph.D. degree in Electrical and Electronics Engineering from VSS University of Technology, Burla, India and Electrical Engineering at Indian Institute of Technology, Delhi, New Delhi, India in 2014 & 2018, respectively. He has worked as a Visiting Student with the Department of Electrical and Electronics Engineering in Cardiff University, UK in 2017. Prior to completion of his PhD, he worked as a postdoctoral researcher in the Department of Electrical and Computer Engineering in National University of Singapore during 2018-19 and in Aalborg University (AAU), Denmark during 2019-2020. He is currently an Assistant Professor in the Department of Energy Technology, AAU, Denmark. He is a recipient of the Indian National Academy of Engineering (INAE) Innovative Students Project Award for his PhD thesis across all the institutes in India for the year 2019. He was also a distinguished reviewer for IEEE Transactions on Smart Grid in the year 2020. He currently serves as a secretary of IEEE Young Professionals Affinity Group, Denmark and Joint IAS/IES/PELS in Denmark section. His research interests are control, optimization, and stability of power electronic dominated grids, renewable energy integration, physics-informed AI tools for cyber-physical power electronic systems.

Mateo D. Roig Greidanus received the B.S. and M.S degree in electrical engineering from the Federal University of Santa Catarina (UFSC) Florianópolis, Brazil, in 2018 and 2020, respectively. He is currently working toward a Ph.D. degree in electrical and computer engineering at the Laboratory for Energy & Switching-Electronic Systems (LESES) with the University of Illinois Chicago (UIC), Chicago, IL, USA. His research interests are modeling, optimal control, non-linear analysis, and stability of power electronic systems, renewable energy integration, and cyber-physical security of power electronic dominated grids.

Frede Blaabjerg (S'86–M'88–SM'97–F'03) was with ABB-Scandia, Randers, Denmark, from 1987 to 1988. From 1988 to 1992, he got the PhD degree in Electrical Engineering at Aalborg University in 1995. He became an Assistant Professor in 1992, an Associate Professor in 1996, and a Full Professor of power electronics and drives in 1998. From 2017 he became a Villum Investigator. He is honoris causa at University Politehnica Timisoara (UPT), Romania and Tallinn Technical University (TTU) in Estonia.

His current research interests include power electronics and its applications such as in wind turbines, PV systems, reliability, harmonics and adjustable speed drives. He has published more than 600 journal papers in the fields of power electronics and its applications. He is the co-author of four monographs and editor of ten books in power electronics and its applications. He has received 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 2014, the Villum Kann Rasmussen Research Award 2014, the Global Energy Prize in 2019 and the 2020 IEEE Edison Medal. He was the Editor-in-Chief of the IEEE TRANSACTIONS ON POWER ELECTRONICS from 2006 to 2012. He has been Distinguished Lecturer for the IEEE Power Electronics Society from 2005 to 2007 and for the IEEE Industry Applications Society from 2010 to 2011 as well as 2017 to 2018. In 2019-2020 he served as a President of IEEE Power Electronics Society. He has been Vice-President of the Danish Academy of Technical Sciences. He is nominated in 2014-2020 by Thomson Reuters to be between the most 250 cited researchers in Engineering in the world.

Jinan Zhang received the B.S. degree from North China Electric Power University in 2012 and M.S. in Electrical Engineering from Tianjin University, Tianjin, China, in 2015. Currently he is pursuing a Ph.D. degree with the University of Georgia, Athens, GA, USA. He is also a Research Assistant with the University of Georgia, USA. His current research focuses on security and resilience in power-electronics-based power systems.

Lulu Guo is with the Department of Control Science and Engineering, and Shanghai Research Institute for Intelligent Autonomous Systems, Tongji University, Shanghai, China (e-mail: guoll21@tongji.edu.cn).

Lulu Guo received the B.S. degree in vehicle engineering and the Ph.D. degree in control engineering from Jilin University, Changchun, China, in 2014 and 2019, respectively. He is currently a senior researcher with Tongji University, Shanghai, China. Before joining Tongji University, he was a Postdoctoral Research Associate with the University of Georgia, Athens, GA, USA. His current research interests include advanced vehicle control, energy management, and vehicle cybersecurity.

Bohyun Ahn (S'17) received the B.S. and M.S. degrees in electrical engineering from Minnesota State University-Mankato in 2016 and 2018, respectively. He is currently pursuing his Ph.D. degree at Texas A&M University-Kingsville. His current research interests include cyber-physical security for distributed energy resources and industry control systems.

Mohammad B. Shadmand (M'15-SM'20) received the Ph.D. degree in electrical engineering from Texas A&M University, College Station, TX, USA, in 2015. From 2015 to 2016, he was an Instructor with the Department of Electrical and Computer Engineering, Texas A&M University. From 2016 to 2017, he was a Research Engineer with the Renewable Energy and Advanced Power Electronics Research Laboratory, College Station, TX, USA. From 2017 to 2020, he was an Assistant Professor with the Department of Electrical and Computer Engineering, Kansas State University, Manhattan, KS, USA. Since 2020, he is an Assistant Professor with the University of Illinois at Chicago, IL, USA. He has published more than 100 journal and conference papers. His current research interests include distributed self-learning control schemes, advanced model predictive control, grid-following and grid-forming inverters, and intrusion detection system for power electronics dominated grids. Dr. Shadmand was awarded Michelle Munson Serban Simu Keystone Research Scholar, Kansas State University in 2017. He was awarded the 2019 IEEE Myron Zucker Faculty-Student Research Grant. He has awarded multiple best paper awards at different IEEE conferences. He has served as Technical Program Co-Chair of the 2019 and 2022 IEEE Smart Grid & Renewable Energy Conference. He serves as Associate Editor of IEEE Transactions on Industrial Electronics, IEEE Transactions on Industry Application, and IET Renewable Power Generation.

Nanditha Gajanur received her B.Tech degree in Electronics Engineering from Manipal Institute of Technology, India in 2017, and M.S degree in Electrical and Computer Engineering from the Ohio State University, USA in 2019. She is currently working toward a Ph.D. degree in Electrical and Computer Engineering at the Laboratory for Energy & Switching-Electronic Systems (LESES) with the University of Illinois Chicago (UIC), USA.

Mohammad Ali Abbaszada (Student Member, IEEE) received the B. Sc. and M. Sc. degrees in electrical engineering from the Ferdowsi University of Mashhad, Iran, in 2017 and 2020, respectively. He is currently working toward a Ph. D degree with Laboratory for energy and Switching-Electronics Systems, University of Illinois at Chicago, Chicago, IL, USA. Since 2018, he has been working on developing different DC Converters. He is currently involved in Inverters and improving the resiliency and reliability aspect of Active Neutral Point Clamped Inverter. His research interests include design and hardware realization of highly efficient and compact power electronics converters and PV inverters, power quality, and hardware realization.