An Overview of Cyber-Resilient Smart Inverters Based on Practical Attack Models

BoHyun Ahn, *Graduate Student Member, IEEE*, Taesic Kim, *Senior Member, IEEE*, Seerin Ahmad, *Graduate Student Member, IEEE*, Sudip Kumar Mazumder, *Fellow, IEEE*, Jay Johnson, *Senior Member, IEEE*, H. Alan Mantooth, *Fellow, IEEE*, and Chris Farnell, *Senior Member, IEEE*

***Abstract*—With high penetration of distributed energy resources (DERs), power systems are increasingly transforming into distributed power grids, which provide grid automation, decarbonization, and decentralization of critical assets. Smart inverters are key power-electronic devices that connect renewable energy and energy storage equipment to power grids. DER includes several intelligent grid functions, such as fault ride through, grid-voltage support, and reactive-power compensation, typically with real-time remote access, data exchange, and seamless over-the-air firmware updates in a cyber-physical environment. However, cybersecurity concerns arise due to extensive information exchange among DER and multiple stakeholders (e.g., utilities, aggregators, vendors, operators, and owners). Therefore, smart inverters account for a growing attack surface for the power grid. This article reviews the cybersecurity best practices and current recommendations for smart inverters and explores emerging cyber threats for smart inverters, including malware attacks and hardware attacks. Finally, we propose a new smart inverter security and resilience framework for developing cyber-resilient smart inverters against the advanced/future threat actors. This article establishes a resilience-by-design baseline reference for smart inverter cybersecurity teams, which bridges the gap between cybersecurity and power-electronics' communities.**

***Index Terms*—Cyberattack, cybersecurity, distributed energy resources (DERs), security-by-design, smart inverter.**

I. Introduction

With the technological advancement of grid automation and the nation's decarbonization and energy security improvement goals, today's electric power grid is transforming to utilize more distributed energy resources (DER), such as photovoltaic (PV) systems, wind energy systems, energy storage systems (ESSs), and electric vehicle charging systems [1], yielding cyber-physical transition [2]. For instance, the capacity of solar is anticipated to grow from 3% (80 GWac) of total U.S. electricity to 40% (1000 GWac) by 2025 and 45% by 2050 (1600 GWac) [3]. Meanwhile, the high penetration of DER has caused grid system instabilities due to their intermittent power generation and low system inertia [4]. To increase the hosting capacity, grid responsiveness, and interoperability of DER, IEEE standards and grid codes have been updated to mandate DER to provide power grid supporting functions (e.g., IEEE 1547-2018 [5] and IEEE 1547.1-2020 [6]) using smart inverters that communicate with utility control and automation systems via standard communication interfaces (e.g., IEEE 2030.5, IEEE 1815, and SunSpec Modbus). Geographically dispersed DER with diverse communication and computation systems is expected to further improve the power grid resilience when coordinated with the power system management [7].

Meanwhile, significant cybersecurity threats have arisen due to extensive information exchanges between DER and multiple stakeholders [8], [9] (e.g., utilities, third-party DER aggregators, vendors, and operators/owners) to manage the DER interconnected with electric power systems, which will expand the power grid attack surfaces compared with other utility-owned power devices (e.g., smart meter and advanced metering infrastructures (AMIs) [10]. Specifically, residential and commercial DERs are further exposed to cyberattacks if connected to poorly secured home/building networks [10], [11]. Various attacks could be ranked in DER systems from a low grid impact on a single residential DER to a high grid impact on large-scale coordinated DER, which, in turn, results in damaging expensive assets, threatening human safety, and substantial disturbances to the distribution power grid operation [10].

A standout real-world threat of DER is an advanced persistent threat (APT) group who is well-resourced and trained threat actors and enables to disrupt/destroy a target system using intelligent techniques, including advanced tools, stealthy approaches, repeated attempts, and long-term attacks [12]. In 2015, a complex cyberattack, including BlackEnergy malware, KillDisk malware, and denial of service (DOS) attack, targeted Ukraine's power grid where an APT group (i.e., Sandworm) switched OFF 30 substations, which left 225 000 people without

Manuscript received 4 September 2023; revised 16 November 2023; accepted 7 December 2023. Date of publication 14 December 2023; date of current version 16 February 2024. This work was supported in part by National Science Foundation under Award CNS-2219733 and Grant 2219734, in part by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy under the Solar Energy Technologies Office Award DE-EE0009026, and in part by the U.S. Department of Energy's Award number DECR0000019. Recommended for publication by Associate Editor Q. Shafiee. *(Corresponding author: Taesic Kim.)*

BoHyun Ahn, Taesic Kim, and Seerin Ahmad are with the Department of Electrical Engineering and Computer Science, Texas A&M University-Kingsville, Kingsville, TX 78363 USA (e-mail: bohyun.ahn@students.tamuk.edu; taesic.kim@tamuk.edu; seerin.ahmad@students.tamuk.edu).

Sudip Kumar Mazumder is with the Department of Electrical and Computer Engineering, University of Illinois Chicago, Chicago, IL 60607 USA (e-mail: mazumder@uic.edu).

Jay Johnson is with DER Security Corp., Scott Valley, CA 95066 USA (e-mail: jay@dersec.io).

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

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TPEL.2023.3342842.

Digital Object Identifier 10.1109/TPEL.2023.3342842

power [13]. In December 2016, a sophisticated multicomponent malware (i.e., Industroyer/Crashoverride, a variant of Stuxnet worm [14]) designed to disrupt industry control systems (ICSs) was discovered, which caused significant power grid outage in Ukraine again [15]. First cyberattack on the U.S. grid was reported on March 5, 2019 [16]. A DOS attack by an unknown threat actor disabled Cisco Firewalls running adaptive security appliance connected to power grid control systems in Utah, Wyoming, and California. The DER operators were temporarily blind to 500 MW wind and solar sites. In 2022, two German wind companies were attacked by ransomware gangs resulting in disconnection to remote monitoring and operation of wind turbines [17]. Eclypsium cybersecurity company revealed that the Conti ransomware APT group who attacked Nordex Group by injecting firmware malware directly into a device-level component, such as a serial peripheral interface (SPI) flash memory [18]. Beginning in April 2022 and continuing through June 2022, the TA423 APT group performed espionage activities in Australian offshore wind turbine entities [19]. Lessons learned from the real-world incidents in power grids include the following.

1) The sophisticated threat actors have been expanding their targets from bulky power plants and substations to DER control systems.
2) Ransomware attacks are the fastest growing form of cyberattacks.
3) Firmware malware attacks can directly target DER devices, including smart inverters.
4) Cyberattack tactics and techniques frequently have evolved, evading the existing DER cyber defense mechanisms.

To address emerging DER cybersecurity concerns, significant efforts have been made by government agencies and power industries. IEC 62351 contains a provision to ensure the integrity, authenticity, and confidentiality of different protocols used in power systems, specifically IEC 62351-12 [20]. Cybersecurity roadmaps for PV systems [21] and wind systems [22] were released in 2017 and 2020, respectively. The roadmaps summarized cybersecurity best practices, looking into the future, and a list of possible next steps for strengthening cyber resiliency. Sandia National Laboratories (SNLs) investigated three advanced network-based defense techniques for DER, including network segmentation, encryption, and moving-target defense in a virtualized environment [23]. SNL sequentially provided recommendation documents for DER network security [24], [25], access controls [26], software patching requirement [27], and requirements of a DER cybersecurity standard [28]. National Renewable Energy Laboratory (NREL) introduced the certification process with 11 test cases for DER networks [29] in 2019 and, subsequently, NREL and UL proposed the UL Cybersecurity Certification Standard for distributed energy and inverter-based resources [30] in January 2023. Starting on February 22, 2019, California Rule 21 mandates that a new DER must be ready to communicate to the host utility using IEEE 2030.5 standard that includes the requirement of transport layer security (TLS) 1.2 [31]. This process can improve network protection against eavesdropping and replay through TLS encryption, man-in-the-middle (MITM) security risk, and spoofing through the security certificates (node authentication). SunSpec Alliance currently provides SunSpec Certified program taking an approach to compliance testing with SunSpec public key infrastructure (PKI), and IEEE 2030.5 network protocol through SunSpec-authorized test labs for DER project, including smart inverters compliance to the California Rule 21 and Common Smart Inverter Profile (CSIP) standard [32]. Currently, a new IEEE 1547.3-2023 [33] (Guide for Cybersecurity of DERs Interconnected with Electric Power Systems) was released in 2023 to fill the DER cybersecurity gap, which includes necessary and optional recommendations. It is anticipated that DER manufacturers should design DER devices, including smart inverters, based on IEEE 1547.3, and DER stakeholders are recommended to follow their roles and responsibilities. In view of this, the adoption of the DER cybersecurity recommendations in design phases is expected to mitigate well-known cyberattacks in ICS or operational technology (OT) systems. As attackers are always evolving new attack techniques and tactics, defensive cybersecurity capabilities must also progress. Therefore, standardization should be only considered as a means for establishing a baseline security level.

Recently, smart inverter cybersecurity research has investigated potential cyberattacks on DER control systems and smart inverters. In 2016, an attack resilient framework for DER was proposed based on the potential vulnerabilities and cybersecurity challenges of multiparty environments [10]. Sebastian and Han [34] explored emerging cybersecurity risks from smart inverters and demonstrated a firmware dumping attack on a commercial smart inverter in 2017. The authors in [35] and [36] introduced cybersecurity vulnerabilities of smart inverters and their impacts on power system operation. Real-time firmware security of smart inverters against controller-firmware modification has been studied [37], [38], [39]. In [39], a power-router prototype using a dual-controller design was proposed to improve uptime and controller-firmware security. Real-time intrusion detection methods have been widely studied to detect forged data (e.g., sensor data and PQ setpoints used for DER inverter controllers) using signature/rule-based network intrusion detection [40], data-driven/artificial intelligence (AI) based method [41], model-based methods [42], and signal process methods (e.g., water marking [43]). Furthermore, the DER controller equipped attack resiliency against sensor data, and the control command modification was proposed to ensure that the grid can remain operational during an attack [44], [45]. A comprehensive survey on potential attack models and defense methods for smart inverters is provided in [46].

Existing literature on DER cybersecurity does not incorporate best practices from the smart inverter industry and DER security standards/recommendations. This article aims to provide a comprehensive review and gap analysis of security best practices based on the reverse engineering of a commercial smart inverter system and security recommendations for the DER industry. In addition, practical cyberattacks on the security-enhanced smart inverters incorporating the current security recommendations are suggested. Finally, we propose a smart inverter security and

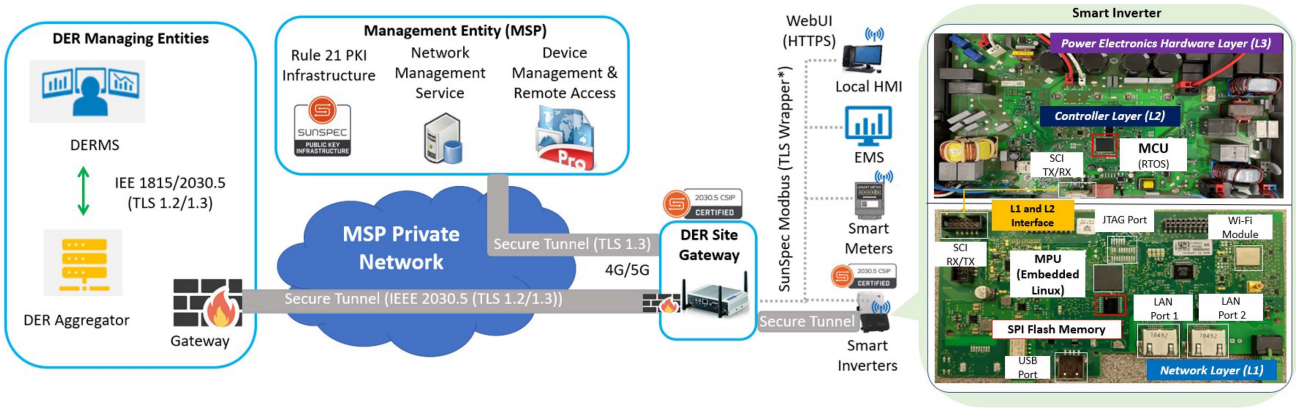


Fig. 1. Practice architecture of the DER system incorporating smart inverters.

resilience framework and discuss future directions for developing a next-generation cyber-resilient smart inverter security by design.

The main contributions of this article can be summarized as follows.

1) We provide a comprehensive review of the latest smart inverter cybersecurity best practices, standards/recommendations, and the latest defense methods.
2) We identify remaining issues, vulnerabilities, and their criticality by reverse engineering an industry-leading smart inverter and assessing current security recommendations for smart inverters.
3) We suggest practical smart inverter attack models based on the remaining issues and identified vulnerabilities of the current best practices and recommendations, and the impacts of the attacks if successful.
4) We propose a new smart inverter security and resilience framework as a practical guideline to achieve device-level security and resilience by design and to leverage developing cyber-resilience for other edge controllers in ICS/OT infrastructures.
5) We provide remaining challenges and future works for industry adoption of the new framework toward cyber-resilient smart inverter.

II. Security Assessment of a Commercial Smart Inverter and Current Recommendations

This section describes the operations of a DER system, reviews cybersecurity features in a commercial smart inverter by reverse engineering, and identifies the remaining vulnerabilities of the current smart inverter cybersecurity recommendations.

A. DER Cyber System

Fig. 1 shows a practice architecture of a DER system incorporating smart inverters, which meets the requirements in California Rule 21. A third-party DER aggregator manages a group of small DER devices on behalf of the DER owners while communicating with utility DER management system (DERMS). A DER site gateway is SunSpec Certified IEEE 2030.5 gateway (e.g., [47]), which is used to interconnect DER devices with a third-party DER aggregator or directly with a DERMS over IEEE 2030.5. CSIP-certified IEEE 2030.5 gateways help the DER managing entities monitor and control DER regardless of the communication capability of the DER devices. Typically, these are IEEE 2030.5 clients that communicate with the DER equipment. The management entities (e.g., PKI servers for certificate management; network management service; vendors and DER site operator/owner for DER device management and maintenance, such as firmware update) can remotely communicate with the DER devices (e.g., smart inverters and DER gateways) using the communication protocols defined in IEEE 1547-2018 (e.g., SunSpec Modbus, DNP3, and IEEE 2030.5) and proprietary network protocols (e.g., HTTPS and 4G/5G cellular network). Smart inverters can be locally accessed by local human–machine interface [e.g., smart inverter user portal (e.g., web user interface (WebUI) with HTTPS)] and local network protocols (e.g., SunSpec Modbus).

B. Smart Inverter

A smart inverter (e.g., [48]) mainly consists of three layers: Network Layer (L1), Controller layer (L2), Power Electronics (PE) Hardware Layer (L3), as shown in Fig. 1. Network layer board L1 includes the following: a microprocessor unit (MPU) with ARM architecture that has relatively high computational power with ROM bootloader and operates smart inverter applications with embedded Linux OS; an SPI flash memory that stores bootloaders (e.g., U-Boot) and a root file system; and additional peripheral network components and interfaces, such as local area network ports, a Wi-Fi module, a USB, a serial communication interface module, and a JTAG debug port. L1 is similar to a typical Internet of Things (IoT) edge device enabling direct connection to external servers in a secure tunnel with TLS 1.2/1.3 via public Internet. Moreover, users/installers also enable to access the smart inverter through a built-in WebUI over Wi-Fi or Ethernet. Control layer board L2 has a microcontroller unit (MCU) that provides relatively lightweight computing power for signal processing and inverter control with a real-time operating system installed in the on-chip MCU memory. Controller firmware is installed in the MCU and updated through L1 or directly through a JTAG debug port in L2. L3 includes PE

TABLE I
REVIEW OF CYBERSECURITY FEATURES FOR COMMERCIAL SMART INVERTER AND CURRENT RECOMMENDATIONS

Feature	Commercial Smart Inverter	Current Recommendations [32], [33]	Defense Mechanisms	Example Issues or Vulnerabilities that Impact the Mitigative Recommendation
1. Secure End-to-End Communication	TLS 1.2/1.3 (encryption with X.509v3 node authentication)	R1. TLS 1.2/1.3 [33] (with PKI [32]) over public internet	D1. Data-in-transit attack prevention (e.g., eavesdropping, replay, and MITM attacks)	V1. PKI vulnerability in TLS (CVE-2015-8960) [53]
2. Secure Local Network [49]	Network service access for only authorized users, Access restrictions in Modbus registers	R2. SunSpec Modbus with TLS wrapper for local network [33] R3. Network segmentation [33]	D2. Data-in-transit attack prevention (e.g., eavesdropping, replay, and MITM attacks), D3. Lateral network movement prevention	V1. PKI vulnerability in TLS I1: Additional network delay affecting inverter control [54], V2. Password vulnerability of smart inverter portal through a local connection V3. Authorized network masquerading [55]
3. Firmware Patching and Booting Security	*R4. Firmware file packing (with obfuscation), Boot (e.g., U-Boot bootloader), CRC integrity checking (checksum), Manual patching	R5. Secure boot [32] R6. Codesigning (replacing CRC integrity checking) [33], R7. Remote patching management [33]	D4. Firmware file reverse engineering prevention, D5-6. Unauthorized firmware modification prevention, D7. Firmware and setting recovery	V4. Advanced unpacking tools [56], V5. U-Boot vulnerabilities (CVE-2022-30790 and CVE-2022-30552) [57], V6. Spoofed code-signing certificate (CVE-2020-0601) [58], Vendor's code signing system vulnerability (e.g., SolarWinds supply chain attack [59]) V7. Disabling remote patching function by malware
4. Device Authentication and Encryption	Manufacturer model OID and serial number for commissioning	R8. Cryptomodule/processor (e.g., TPM chip) [33]	D8. Data-at-rest falsification prevention, stealing private/secret key prevention	V8. TPM vulnerability (CVE-2018-6622) [60]
5. Device Access Control	Firewall (blacklist) in a router/gateway, ID and password	R9. Firewall with whitelist in a router/gateway [33] R10. (Password-based) MFA [33] R11. Role-based access control [33]	D9-11. Unauthorized device access prevention	V9. IP masquerading [55], V10. MFA prompt bombing [61] V9-11. Insider [62], I2: Need a zero-trust-security
6. Device-Level IDS [50]	Audit/log records	R12. Network-based IDS including deep packet inspection in the DER site network gateway [33]	D12. Network attack detection (e.g., DOS attack, unauthorized access, eavesdropping, relay, and MITM)	V12. Local network vulnerability and device access control vulnerabilities; I3. Need a device-level IDS best practices and standard
7. Malware and Ransomware Security [51]	Not specific method found beyond the firmware and booting security	R6-7. Firmware security [33], R12. Network IDS R13. Physical access factory reset [33]	D13. Malware tampered smart inverter recovery	V4-6. Firmware patching and booting vulnerabilities, V7. Disabling remote patching function, V13. long recovery time, stolen confidential data will bring chances to the next ransomware attacks [63], I4. Need malware security best practices and standard
8. Hardware Security [52]	R14. Debugging for only authorized users Disabled USB, Serial, JTAG, etc. debug interface	R14. Disabling debug interfaces and ports [32] R15. Supply chain security [33]	D14. Firmware modification/malware prevention through debug interfaces, D15. Counterfeit IC chips prevention	V14. Reactivating debugging interface [64], V15. Side-channel attacks and advanced HTR [65] I5. Need a hardware security best practice and standard
9. RC [20]	Not specific method found	**Not specific inverter-level method found [32], [33], [20], [49], [50], [51]	N/A	I6. Need resilient control best practices and standard addressing specified attacks

R#: Currently recommended security functions; D#: Defense mechanism corresponding to R#; V#: Vulnerability corresponding to R#, I#: Identified issues
* It is noted that R4 was not listed in current standards/recommendations ([20], [32], [33], and [49], [50], [51].

hardware components, such as power switches, gate drives, relays, analog filters, sensors, and communication interfaces with L2.

C. Security Assessment of Commercial Smart Inverter Security and Current Security Recommendations

In this article, a total of nine security features are selected based on the IEEE 1547.3 [33], SunSpec DER Device Security Certificate (Phase 1) [32], IEC 62351-12 [20], and other cybersecurity guidelines, such as UL certification [30], [49], [50], [51], [52], to review a commercial smart inverter. Table I presents the summary of smart inverter cybersecurity features for an industry-leading commercial smart inverter and current recommendations. Typical defense mechanisms (D#), including prevention, detection, and recovery, were used to assess the current security functions (R#). It is expected that R# can improve the security level of the current DER smart inverters and potentially pass the security certification tests, such as NREL/UL certification [30] and SunSpec DER Device Cybersecurity Certification [32]. However, the smart inverters with R# will still be vulnerable to advanced attack tactics and threat actors, such as insiders, which were expressed as V#. Identified issues were expressed as I#. Besides, the criticality of the existing vulnerabilities is assessed in the Appendix.

Network Security: The commercial smart inverter utilizes TLS 1.2/1.3 encryption with X.509v3 node authentication for Internet-routed communications over the public Internet between an external server (e.g., vender server) and the smart

inverter (i.e., HTTPS) (R1) and enables DER network protocols, such as IEEE 2030.5 communication, externally over the Internet. SunSpec Modbus communications with access limited Modbus registers over the public Internet or local network can be secure by incorporating a TLS wrapper (R2), as (SunSpec) Modbus has no encryption and authentication functions [33]. These can prevent major data-in-transit security concerns, such as eavesdropping, reply, and MITM attacks in the DER network (D1). However, Dai et al. [53] discovered and demonstrated that fake certificates issued by a DNS cache poisoning could compromise existing PKI technology in TLS (V1). In addition, an occurrence of network delay in the DER facility operation [54] can be challenging if TLS is adopted in the local Modbus communication (I1). Also, password stealing of a smart inverter portal through a local connection (e.g., keylogging) will open a door for modifying Modbus registers, which bypasses security rules in restricted access registers and TLS security (V2). Even though the current smart inverter provides local network service access and for only authorized users [49], the network segment method (R3) can be applied to distribute data into multiple protected zones and prevent lateral network movement [33]. However, an authorized network masquerading as normal-looking network access can bypass the existing security rules in the network segment framework (V3) [55].

Firmware Patching and Booting Security: It is observed that the available firmware used to update the commercial inverter is packed with obfuscation methods (R4), such as compression and encryption, to prevent unauthorized firmware file reverse engineering (D4). However, advanced unpacking tools and methods can unpack the firmware file [56] and conduct file reverse engineering (V4). Secure boot (R5) checks the authenticity and integrity of the firmware (e.g., bootloader, Linux kernel, and Root file system) during the boot process, which is a crucial chain of trust for firmware booting security (D5). However, selecting a secure implementation is critical because multiple U-Boot vulnerabilities were found recently (CVE-2022-30709 and CVE-2022-30552 [57]) (V5). Furthermore, the cyclic redundancy check (CRC) method checks software/firmware integrity during firmware update/booting process in the commercial smart inverter. In [33], the codesigning method (R6) is recommended that utilizes a cryptography signing key and hash integrity checking instead of the checksum-based CRC method, which can prevent unauthorized firmware modification (D6). However, the codesigning could be vulnerable to a spoofed codesigning certificate (CVE-2020-0601) [58] and vendor's codesigning system vulnerability (e.g., SolarWinds supply chain attack [59]) (V6). When attackers breach codesigning systems, they can update malicious firmware as the authorized patching process.

Device Authentication and Encryption: The commercial inverter uses its manufacturer model object identifier (OID) and serial number during the commissioning process without evidence of the use of a cryptomodule/process. Therefore, appending a cryptomodule/process (R8) is recommended in [33], such as a trusted platform module (TPM) chip that generates and securely manages secret/encryption keys. The cryptomodule can prevent data-at-rest falsification by attesting the data hash (D8). However, vulnerabilities on a TPM chip could leak secret keys (V8) [60].

Device Access Control: The inverter offers a blacklist-based firewall in a router/gateway and requires a user ID and password to access the smart inverter (e.g., WebUI over Wi-Fi or Ethernet). Meanwhile, the standard recommends the use of a whitelist firewall (R9), a password-based multifactor authentication (MFA) (R10) to prevent password-guessing attacks, and a role-based access control (R11) [33]. These will prevent unauthorized device access (D9–D11). Historically, access control functions are vulnerable to IP masquerading (V9) [55] and MFA prompt bombing (V10) to trick users into letting them in [61]. Moreover, insiders (e.g., disgruntled employees or malicious insiders) (V9–V11) can have an access privilege as authorized vendors or operators, which can bypass any security functions by disgruntled employees [62].

Device IDS: The smart inverter provides an audit/log record system as IDS [50], while the standard recommends a network-based gateway IDS with a deep packet inspection in the DER site network gateway for the device-level IDS (R12) [33]. However, the smart inverter will be threatened by existing vulnerabilities, such as the local network vulnerabilities and device access control vulnerabilities and malware attacks (V12). Therefore, an inverter host-based IDS guide should be further developed.

Malware and Ransomware Security: Because malware and ransomware can be loaded to smart inverters via network, current smart inverter vendor may provide network-based IDS or IPS [51]. However, no specific malware and ransomware security methods were found beyond the firmware and booting security in the smart inverter (R6 and 7). The local factory reset (R13) could be used if remote patching was disabled by malware or ransomware [33]. However, a long recovery time is anticipated due to the manual recovery process by physical access (V13). Besides, stolen confidential data from the smart inverter will increase the chances of the next ransomware attacks [63].

Hardware Security: Typically, debug interfaces are allowed for authorized personnel [52]. However, we observed that the JTAG debug interface of the inverter was disabled (R14), which prevented firmware modification by physical access (D14). However, a reverse firmware engineer demonstrated reactivating the debugging interface (V14) [64]. Although the overall concept of supply chain security (R15) can mitigate counterfeit IC chip attacks (D15) [33] and the side-channel attacks, advanced hardware trojan (HTR) at each stage of the IC supply chain and printed circuit board (PCB) level trojan are the threats of disrupting the hardware (V15) [65].

Resilient Control (RC): The edge DER control is responsible for rapidly generating the desired control sequences for the DER converters guided by local measurements and global consideration, including the coordination. Furthermore, implementing robust resilience for mission- and time-critical operation of DER is a critical challenge facing DER-based resilient power systems. RC function for DER smart inverters was not found in the smart inverter and current DER cybersecurity standard/recommendation.

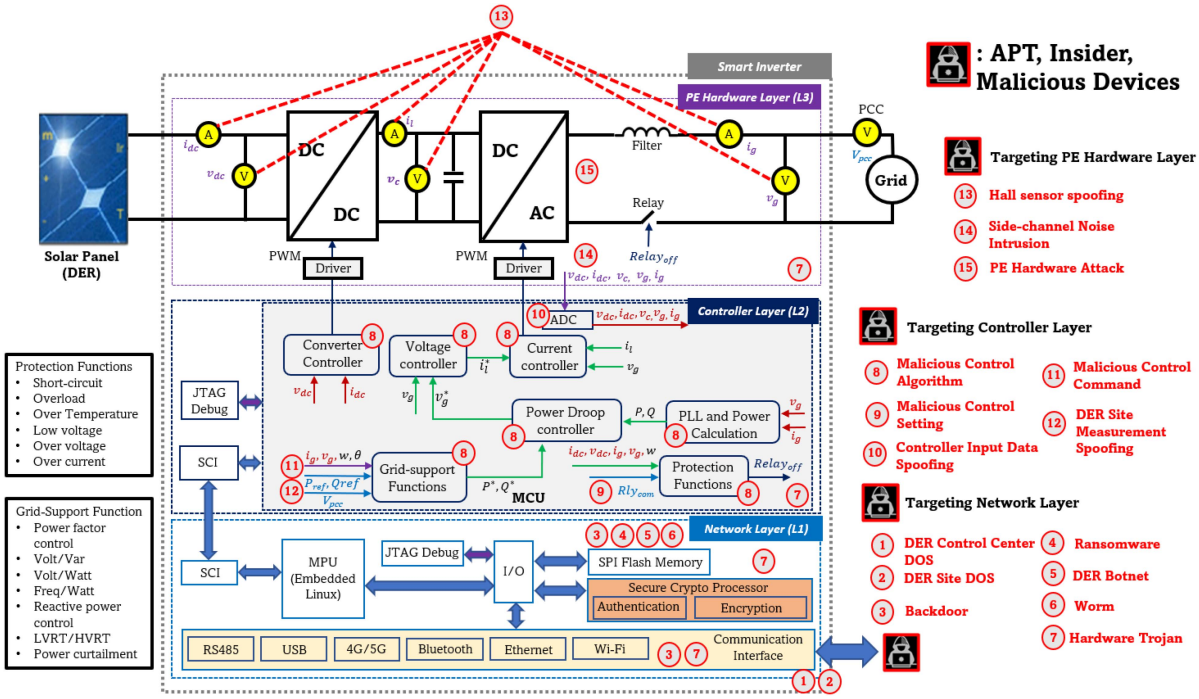


Fig. 2. Practical cyberattack model targeting security-sensitive layers of a smart inverter.

Overall, the current security best practice and standard/recommendation (the current recommendations) for smart inverters mostly focus on network security and firmware security in the prevention stage, neglecting critical security requirements of the smart inverters, specifically malware, ransomware, RC, and hardware security. In addition, it is anticipated that quantum attacks will be feasible in just five to ten years [66]. If the quantum computing attack is possible, the adversary can easily leverage existing vulnerabilities of V1 (PKI vulnerability in TLS), V6 (Spoofed codesigning certificate), V7 (TPM vulnerability), and V10 (MFA) by extracting private keys or predicting passwords [66]. It is noted that the vulnerabilities in Table I are just examples. New vulnerabilities can be discovered and used by adversaries. From a security design perspective, it is assumed that such vulnerabilities are successfully used for creating specific attack vectors and lead to success in developing practical attack models.

III. Practical Attack Modeling Targeting Smart Inverter and Impacts

In this section, we introduce practical attacks targeting specific layers of the smart inverter with the recommended security functions, as described in Section II. Fig. 2 shows the security-sensitive layers of a smart inverter and potential attacks on the layers and Table II summarizes the security threat modeling of the smart inverter. A total of 15 practical attack models are suggested based on the identified vulnerabilities and real-world incidents and the impacts of the attack models are discussed.

A. Network Layer Attacks

Attack #1—DER Control Center DOS Attack: DOS/distributed DOS (DDOS) attack disables network communications by intentionally flooding network packets or at a particular time once the IP address and port number of the network device are known to the attacker. The real DOS cyberattack incident that targeted the DER control center demonstrated the capability of communication loss interrupting the DER management service [16]. Ahmad et al. [67] validated an inverter-level impact from a DER control center DOS attack, resulting in a loss of receiving a control command and grid data. Therefore, it can be expected that a DOS attack on a control center that manages DER sites in a region can cause a regional blackout.

Attack #2—DER Site DOS Attack: Choi et al. [68] experimented DOS attacks on a smart inverter and showed impacts on a typical DER site using a hardware-in-the-loop testbed. Two DOS attacks were emulated: TCP ACK flooding DOS attack using Hping3 tool and Packet Drop DOS attack using Ettercap tool to disrupt the local DER site. Once the flooding DOS attack was launched, the MPU and network resource usage rapidly increased, resulting in loss or delayed communication of the smart inverter. Meanwhile, the packet drop DOS attack dropped the network data (e.g., active power data from the smart inverter). The DER control center will have a loss/delay of monitoring and control support of the affected inverters [68]. However, the chance is very low to generate widespread DOS attacks targeting all smart inverters. Therefore, the grid impact is expected to be low compared with the DER control center DOS attack.

Attack #3—Backdoor Attack: Backdoor is a malware attack, and it can be exploited as an initial access and reconnaissance of

TABLE II
SECURITY THREAT MODELING FOR SMART INVERTER

Security Sensitive Layer	Attack Category	Attack Name	Attack Vector/Case (AV#. Attack Vector)	Smart Inverter Impact	Grid Impact (Group of Smart Inverters) by AV#
Network Layer	DOS Attack	1. DER Control Center DOS	AV1. DOS attack targeting DER control system (e.g., network DOS attack [16])	Loss of control command and grid data from the control center [67]	AV1: Regional blackout covered by the DER control center [16]
		2. DER Site DOS	AV2. IP address and port scanning and conduct DOS attack (e.g., TCP ACK or packer drop [68])	Loss or delayed communication [68]	AV2: Loss of affected inverter monitoring and control support [68]; mostly localized grid impact due to the difficulty of creating widespread DOS attacks on each DER site
	Malware Attack	3. Backdoor	AV3. Physical/local access AV4. DER control center/operator-side attack vector (e.g., Conti), AV5. Vendor-side attack vector: Adversary steal codesigning key and sends malware signed by the key [58]	Initial access and explore the smart inverter [12], Privilege escalation, and deactivating security functions [69], Install malware [12], [69]	AV3-5: No direct grid impact
	Malware Attack	4. Ransomware		Remote access functions are encrypted, bricked/malfunctioned [63]	AV3: Localized grid impact, AV4: Reginal grid disturbance, AV5: Widespread negative grid impact
	Malware Attack	5. DER Botnet		Smart inverter is controlled by adversary [70]	AV4-5: Create a DDOS attack targeting the control center or malfunctioning smart inverters causing longer regional blackout
	Malware Attack	6. Worm		Smart inverter continuously propagates automatically evolving malware [71]	AV4-5: Widespread and severe impact and requiring long recovery time
	Hardware Supply Chain Attack	7. HTR	AV6. Trojan IC insertion [65], AV7. PCB trojan insertion [73]	Hardware backdoor steal data and enables the attacker access to Network Layer [72]	AV6-7: Widespread negative grid impact as malware attacks through malicious supply chain
Controller Layer	Controller-Firmware Attack	8. Malicious Control Algorithm	AV8-10. Malicious controller firmware is patched to the controller after it was loaded to the Network Layer first like the malware attack vector AV3-5, respectively [74]	Inverter controller maliciously operates or operates counter to grid operator commands [76]	AV8: Localized grid impact AV9: Regional grid disturbance [76], AV10: Wide area grid disturbance [76]
		9. Malicious Control Setting	AV11. Control setting is compromised through Edit Parameters or Parameter File update by malicious (grid) operator AV12. Malicious smart inverter user portal	Inverter control settings (e.g., protection setting and ride-through settings) are changed causing inverter tripping during grid disturbance [76]	AV11: Widespread DER inverter tripping during grid disturbance resulting in regional blackout [76] AV12: Localized grid impact
	Controller-Firmware Attack + False Data Injection Attack (FDIA)	10. Controller Input Data Spoofing	AV8-10. Malicious controller firmware is patched	Falsified controller input sensor data will degrade the inverter operation or lead to tripping [77]	AV8: Localized grid impact AV9: Regional grid instability [77], AV10: Cascade tripping and wide area blackout [76]
	MITM + FDIA	11. Malicious Control Command	AV12. Malicious smart inverter user portal AV13. Local MITM AV14. TLS MITM [53] AV15. TLS CA MITM [78]	Inverter operates corresponding to the malicious grid-support command [12]	AV12-13: Localized grid impact AV14: Regional grid disturbance [12], AV15: Wide area grid disturbance
	MITM + FDIA	12. DER Site Measurement Spoofing	AV12. Malicious smart inverter user portal AV13. Local MITM	Inverter performance will degrade [79]	AV12-13: Localized grid impact
PE Hardware Layer	Physical Attack + FDIA	13. Hall Sensor Spoofing	AV16. Physically injecting electromagnet field to Hall sensors [80]	Hall sensor measurement increase during the attack [80]	AV16-18: Appreciable impact (e.g., potentially subsynchronous operation) depending on which control nodes are attacked and at what tampering noise frequency
	Physical Attack + FDIA	14. Side-Channel Noise Injection	AV17. Physically injecting EMI noise to IR light sensor or AC signal to input of ADC [81]	The injected noise can degrade the performance of the inverter control operation or malfunction [82], [83]	
	Physical Attack	15. PE Hardware Attack	AV18. Tampering, swapping, or damaging PE hardware components [84]	PE hardware faults or degrade inverter performance or shut-down by protection circuits [84]	

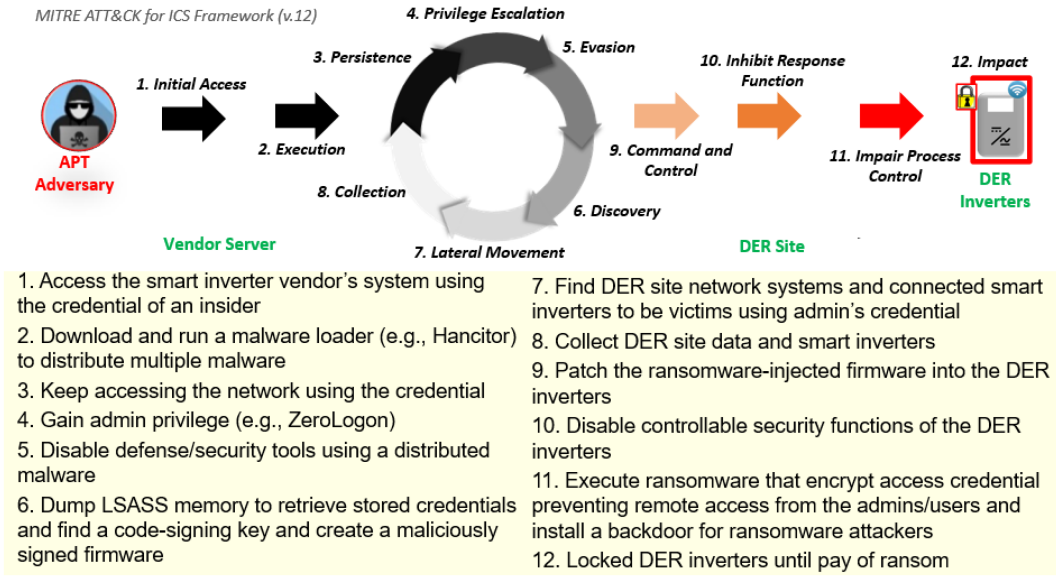


Fig. 3. Ransomware attack model targeting DER smart inverters through an inverter vendor's OTA firmware update system.

a target smart inverter and the connected network devices. For example, a backdoor can be established on the flash memory of the network layer by an insider, masqueraded software [12], or a malicious firmware update using the patching and booting vulnerabilities. Once the backdoor is installed in the smart inverter, the attackers can escalate their privilege and install malware (e.g., ransomware, botnet, and worm) to the smart inverter while bypassing/deactivating the embedded security functions [69].

Attack #4—Ransomware Attack: Ransomware is one of the fastest growing malware types that holds the system for ransom by locking the users from accessing the system (Locker/Blocker-style ransomware) or encrypting their important/credential data of the target system (Cryptostyle ransomware). An example of a ransomware attack model is shown in Fig. 3. A locker-style ransomware attack will encrypt the remote access functions of the smart inverters (e.g., authorized user access credential in "passwd" file) and manipulate the inverters to be bricked/malfunctioned. As a result, DER operators cannot access and control the locked and malicious smart inverters [63] causing the local grid disturbance.

Attack #5—DER Botnet Attack: A DER Botnet (i.e., bot network) is a group of compromised DER devices by botnet malware. Although the DER Botnet has been inactivated for a long time, it will be simultaneously controlled by a single or multiple cyberattackers for coordinated malicious activities at a certain period. For example, the DER botnet can initiate a DDOS attack targeting the DER control centers. Also, DER smart inverters affected by botnet malware can malfunction during specific grid events, which will cause a longer regional blackout [70].

Attack #6—Worm Attack: A worm is a self-replicate, self-propagate, and self-run malware automatically compromising other connected systems via networks [71]. For example, pandemic malware finds and infects all devices on the network in the shortest time possible via a brute force approach. This is distinct from virus, which requires a user's manual execution to initiate replication and propagation. In a DER network system, a compromised smart inverter device or gateway by worm would propagate to compromise other DER devices and the DER control center in the DER network. The worm-infected DER control center and devices may spread worms to the other power grid stakeholders. If the widespread of the worm attack is successful, there will be severe damages to the power grid and the longest recovery time is anticipated since it is unclear how many devices and systems are infected by worms.

Attack #7—HTR Attack: Conventional HTR is a malicious modification of the circuitry of an integrated circuit (IC) and it may target any layers of the smart inverter. For example, a trojan circuit embedded in a chip (i.e., spy chip [72]) on the network layer of the smart inverter can be exploited as a backdoor access. In addition, PCB trojan [73] can be created by tampering the interconnect lines at the internal layers or altering the components, which will cause the leak of secret information about the smart inverter. Such supply chain type attacks will bring widespread negative grid impacts.

B. Controller Layer Attacks

Malicious controller firmware can be delivered via an over-the-air (OTA) updating process to the network layer of the smart inverter first, then it will be patched into the MCU in controller layer [74]. This controller-firmware attack vector will bring Attacks #8, #9, and #10 in a stealthy way.

Attack #8—Malicious Control Algorithm Attack: The smart inverter will operate maliciously due to the modified inverter control algorithms through the controller-firmware modification. For example, the malicious modification of the maximum power point tracking (MPPT) algorithm in the converter control block in Fig. 2 can limit the power generation of the solar inverter [75]. Besides, the smart inverter operates counter to grid-supportive function commands once the grid-support functions block is maliciously modified [76]. As a result, a regional disturbance or blackout can be anticipated.

Attack #9—Malicious Control Setting Attack: The smart inverter control parameters are set to certain values and can be changed to optimize the performance of the inverter by configuration change patch methods. Control setting can be compromised through edit parameters or parameter file updates by malicious grid operator in DER control servers (AV11) or malicious smart inverter portal user (AV12). This attack is a DER control misconfiguration attack leveraging the new required grid-support functions defined in IEEE 1547-2018, such as DER ride-through setting and trip threshold setting, causing inverter tripping during a grid disturbance [76]. The nefarious control setting of multiple inverter-based DER sites can result in a regional blackout.

Attack #10—Controller Input Data Spoofing Attack: This attack spoofs the on-board sensor data used as stealthy inputs of the inverter controller by the firmware modification (AV8–10). If the attacker has no prior knowledge of the system, the on-board sensor data will be designed by mixing the original value with a malicious factor, as $\tilde{y}\ (t) = \ y(t) + \beta$ during the attack duration. Here, β is unknown signal due to the malicious modification of the signals [77]. Falsified controller input sensor data will degrade the inverter operation or lead to tripping [77]. The degraded smart inverters may cause grid instability [77]. In addition, the groups of tripped smart inverters can cause a regional blackout [76].

Attack #11—Malicious Control Command Attack: This attack aims to modify or create malicious control commands, such as grid-support functions and a rapid shut-down for solar systems, from the DER control center to the smart inverters using a malicious smart inverter user portal (AV12) or MITM attack schemes (AV13–15). For example, an MITM tool (e.g., Ettercap) in a DER site network will be installed in a DER site router or data aggregator (AV13. DER site MITM) [12]. An adversary steals TLS certificate key of the DER control center or session keys and then builds an MITM (AV14. TLS MITM) [53]. The smart inverters controlled by the DER control center will maliciously operate, which will cause regional grid disturbance [12]. The worst attack case will be anticipated if the adversary succeeds in manipulating TLS certificate authority (CA) and then builds MITMs verified by the CA among DER control centers and numerous smart inverters (AV15. CA MITM) [78]. Using the CA MITM, malicious control commands can be simultaneously sent to the groups of smart inverters, resulting in wide area grid disturbance.

Attack #12—DER Site Measurement Spoofing: Grid (e.g., V_{pcc}, voltage at point of coupling) and local measurement (e.g., local sensor data) used in the inverter controller can be falsified through the malicious smart inverter user portal (AV12) or local MITM (AV13) [79].

C. PE Hardware Layer Attacks

PE hardware layer exposed to physical access will be a target of attackers. In this article, three types of hardware attacks are considered. Fig. 4 shows an example of attack points targeting the PE hardware layer. Overall, PE hardware layer attacks will cause low grid impact. However, it is anticipated that small drones equipped with an EMP generator may create Attacks #13 or #14 targeting widespread smart inverters.

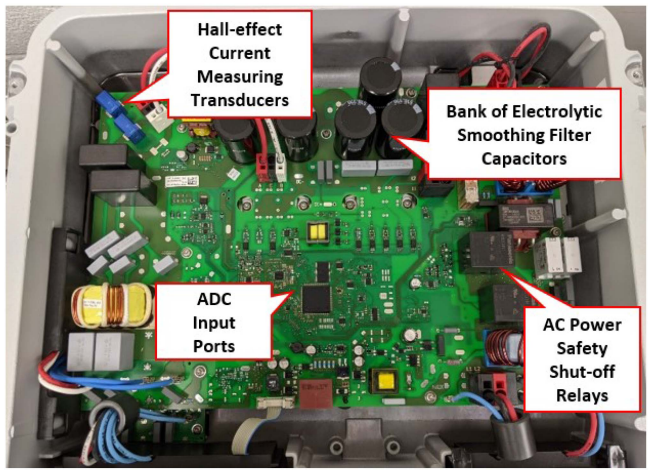


Fig. 4. PE hardware layer attack points.

Attack #13—Hall Sensor Spoofing Attack: This attack is a noninvasive hardware attack targeting hall sensors measuring the voltage and current of the inverter. For example, an attacker physically injects external electromagnetic signals to perturb the magnetic field intensity of the Hall sensors by attaching or placing an electromagnet [80] near the target inverter (AV16). The Hall sensor measurement can be increased during the attack.

Attack #14—Side-Channel Noise Injection Attack: This attack intentionally injects noise signals to manipulate sensor data. For example, intentional electromagnetic interference noise can be induced by the input of analog-to-digital converter (ADC) due to electrostatic discharge diodes or a photo-diode-based infrared (IR) light sensor using an antenna (AV17) [81]. The injected noise can degrade the performance of the inverter control operation or malfunction [81], [82], [83].

Attack #15—PE Hardware Attack: Intentional PE hardware layer attack can include tempering, swapping, and vandalism to defect the PE hardware layer by physical attackers (AV18). This attack can cause degrading inverter performance, PE hardware components' faults, and shutting-down the device by the protection circuits [84].

IV. Cyber-Resilient Smart Inverter Security by Design

This section proposes a smart inverter security framework using additionally recommended defense strategies that are expected to mitigate the challenging attacks, as introduced in Section III, and then discusses remaining challenges and future direction. In general, a cybersecurity framework provides a structured approach to address the cybersecurity requirements of a target system. A popular framework is the National Institute of Standard Technology (NIST) Cyber Security Framework [85], which provides security recommendations for critical infrastructure organizations in each stage, including identify, protect, detect, respond, and recovery. Based on the NIST cyber security framework, four stages are considered for designing a cyber-resilient smart inverter, including prevention, detection,

TABLE III
SMART INVERTER SECURITY AND RESILIENCE FRAMEWORK (PROPOSED RECOMMENDATIONS)

Attack Name	Prevention (*Standard + Design Stage + Proactive Detection)	Detection (Reactive Detection)	Resilience (Incident Response + Fast Recovery)	Forensics (Incident Analysis)
1. DER Control Center DOS	Not a scope of a smart inverter device level	N-ID1. Control Center Down Detection	CRC1. DER DOS RC (e.g., redundant blockchain network [68])	NF1. Control Center Network Forensics
2. DER Site DOS	N-IP1. Standard Network Security (R1-3, R8. PUF-embedded cryptomodule [78], R9–12) N-IP2. PQC-grade Network Protocol	N-ID2. DOS Attack Detection (e.g., cyber data [40], physical data [86], and hybrid [87], [88])	RC1. DOS Attack (e.g., fallback control [89], and prediction policy [86])	NF2. DER Site Network Forensics
3. Backdoor	M-IP1. Standard Firmware Security (R4–7) M-IP2. Malware File Prevention (e.g., antivirus scanning [74], binary Image-based deep learning [69], dynamic malware analysis [90]) M-IP3. PQC-grade Codesigning	M-ID1. General Malware Detection (e.g., HPC-ML[91] and side-channel-based malware detection [92]), M-ID2. Backdoor Detection (e.g., UFO [93]), M-ID3. Ransomware Detection, M-ID4. Botnet Device Detection (e.g., [94]), M-ID5. Worm Device Detection	MR1. General Malware Recovery (e.g., [95])	MF. Malware Forensics (e.g., memory forensics [97])
4. Ransomware			MR2. Ransomware Recovery (e.g., key discovery/backup [96]), CRC2. DER Ransomware	
5. DER Botnet			CRC3. DER Botnet RC	
6. Worm			CRC4. DER Worm RC	
7. HTR	HT-IP. HTR Prevention (e.g., structural checking during testing [98], Obfuscation-based PCB trojan protection [99], and on-chip magnetic probes [100])	HT-ID. HTR Detection (e.g., side-channel analysis [101])	HTR. Hardware Trojan Mitigation	HTF. Hardware Trojan Forensics
8. Malicious Control Algorithm	CF-IP. Malicious controller-Firmware Update Prevention (e.g., [38] and [39])	CF-ID1. Malicious Control Algorithm Detection (e.g., HPC-ML [102])	CFR. Controller-firmware patching (e.g., [38] and [39])	FF. Controller-Firmware Forensics
9. Malicious Control Setting		CF-ID2. Malicious Control Setting Detection (e.g., HPC-ML [102])		
10. Controller Input Data Spoofing		CF-ID3. Controller Input Data Spoofing Detection (e.g., Kalman filter [77])		
11. Malicious Control Command	CC-IP. Malicious Control Command Prevention (e.g., grid code [45] and blockchain [103])	CC-ID. Malicious Control Command Detection (e.g., [45])	RC2. Malicious Control Command (e.g., [45])	NF1
12. External Measurement Spoofing	EM-IP1. Grid Data Spoofing Prevention (e.g., [104]), EM-IP2. Local Sensor Data Spoofing Prevention (e.g., watermarking [105]),	EM-ID1. Grid Data Spoofing Detection (e.g., [41] and [106]) EM-ID2: Local Sensor Data Spoofing Detection (e.g., [42]),	RC3. Grid Data Spoofing RC (e.g., [106]), RC4. Local Sensor Data Spoofing RC (e.g., [44]),	NF1, NF2
13. Hall Sensor Spoofing	PE-IP1. Shielding, PE-IP2. Physical Access Prevention (R13), PE-IP3. PE Hardware Authentication (e.g., RC filter method [107])	PE-ID1 Hall Sensor Spoofing Detection	RC5: Hall Sensor Spoofing RC	PEF. Power-Electronics Hardware Forensics (e.g., [84])
14. Side-Channel Noise Injection		PE-ID2. Side-Channel Noise Injection Detection (e.g., [81])	RC6. Side-Channel Noise Injection RC (e.g., [81])	
15. PE Hardware Attack		PE-ID3. PE Hardware Attack Diagnosis (e.g., [84])	RC7. Fault-tolerant control (e.g., [108])	

resilience, and forensics. Table III presents the proposed smart inverter security and resilience framework with the recommended key defense strategies that need to be included in the future smart inverter cybersecurity standard/recommendation.

Prevention: In addition to the industry standard security functions, as introduced in Section II, intrusion preventions (IPs) are required to prevent the attacks in design stage and protect the smart inverter by proactively detect intrusions, which include standard network prevention (N-IP1: R1–3, R8–12), PQC-grade network protocol (N-IP2), standard firmware security (M-IP1: R4–7), malware file prevention (M-IP2), PQC-grade codesigning (M-IP3), HTR prevention (HT-IP), malicious firmware update prevention (CF-IP), malicious control command prevention (CC-IP), grid data spoofing prevention (EM-IP1), local sensor data spoofing prevention (EM-IP2), shielding (PE-IP1), physical access prevention (PE-IP2: R13), and PE hardware authentication (PE-IP3).

As most smart inverters are resource-constrainted devices, smart inverter developers need to prioritize the IPs based on their security budget and severity. Besides, additional external security system, such as malware file screening server [74] and blockchain security server [103], can be used to support additional computational resources for M-IP1, HT-IP, CF-IP, CC-IP, and EM-IPs, while smart inverters install APIs accessing the external system.

Detection: A smart inverter conducts real-time attack detection if an attack bypasses the prevention tools and impacts the smart inverter (i.e., reactive detection). To effectively detect the practical attacks in Section III, various intrusion detection systems (IDs) are necessary. As per DOS-related attack detection, control center down detection (N-ID1) and DOS attack detection (N-ID2) are suggested. Malware detection algorithms are needed, which include general malware detection (M-ID1), backdoor detection (M-ID2), ransomware detection (M-ID3),

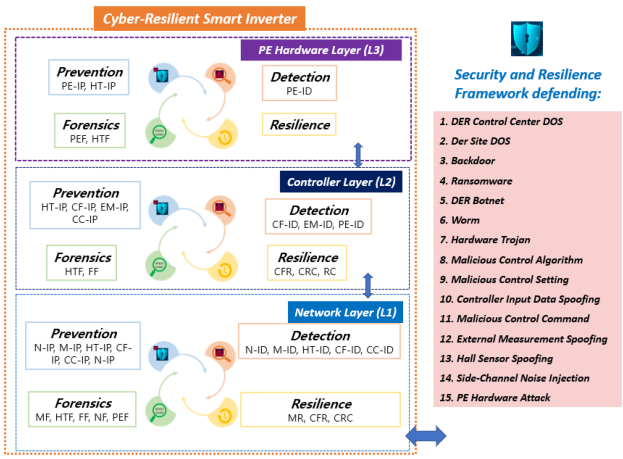


Fig. 5. Cyber-resilient smart inverter security and resilience by design based on the smart inverter security and resilience framework.

botnet device detection (M-ID4), and worm device detection (M-ID5). Besides, HTR detection (HT-ID), malicious control algorithm detection (CF-ID1), malicious control setting detection (CF-ID2), controller input data spoofing detection (CC-ID), malicious control command detection (CC-ID), grid data spoofing detection (EM-ID1), local sensor data spoofing detection (EM-ID2), Hall sensor spoofing detection (PE-ID1), side-channel noise injection detection (PE-ID2), and PE hardware attack detection (PE-ID3) are suggested.

Besides prioritizing detection algorithms, implementation of the reactive detection algorithms requires an additional processor for a comprehensive attack diagnosis leveraging fault/attack location, isolation, and service restoration (FLISR). Furthermore, the results will no longer be trusted if the detection algorithms are implemented in the malware-infected controller/processor.

Resilience: Resilience refers to the ability of the DER smart inverter to promptly respond, withstand, and fast recover from attacks. Control resilience can be achieved by both self-RC for smart inverter resilience and coordinated resilient control (CRC) by a group of smart inverters for grid resilience. RC functions include DOS attack resilient control (RC1), malicious control command resilient control (RC2), grid measurement spoofing resilient control (RC3), local measurement resilient control (RC4), Hall sensor spoofing resilient control (RC5), side-channel noise injection resilient control (RC6), and fault-tolerant control (RC7). Recommended CRC functions for the power grid resilience include DER DOS resilient control (CRC1), DER ransomware resilient control (CRC2), DER botnet resilient control (CRC3), and DER worm resilient control (CRC4). Besides, detailed malware resilience (MR) functions are required, which include general malware recovery (MR1) and ransomware recovery (MR2). Furthermore, fast HTR and controller-firmware patching (CFR) are necessary in resilience stage once the attacks are detected.

Forensics: Forensics stage aims to analyze the evidence of incidents of the smart inverters and evaluate the defense strategies after attacks. The required forensics functions include external network forensics (NF1), DER site network forensics (NF2), malware forensics (MF), hardware trojan forensics (HTF), controller-firmware forensics (FF), and power-electronics hardware forensics (PEF).

The practice of deliberately extracting and preserving data after an intrusion is not yet a supported feature of the smart inverter. Also, it might be difficult to remove a device from the grid for forensics analysis. Additional tools (e.g., forensics designated port) should be considered in the future smart inverter design.

V. Case Study of Smart Inverter Security and Resilience Framework

This section reviews the existing defense strategies that might be adopted to the smart inverter security and resilience framework and the remaining works. Fig. 5 shows a concept of cyber-resilient smart inverter design based on the smart inverter security and resilience framework.

A. DOS Attack Defense (Attacks #1 and #2)

Prevention of Attack #1 might be not a scope of smart inverter device level. With a redundant wide area network, CRC1 can be achieved. In [68], smart inverters use additional BC network to enhance the resilience of DERMS by recovering the operation of a DER system once the DERMS outage is detected. The BC system as a governance platform for the DER system provides security and RC services on behalf of the DERMS until the availability of the DERMS is recovered.

Overall, network attacks can be mitigated by N-IP1 and N-IP2. Specifically, physically unclonable function (PUF) embedded cryptomodule providing robust key protection against physical intrusion and reverse engineering attacks protect private keys [78] and upgrading PKI cryptography algorithms with post-quantum cryptography (PQC)-grade algorithms can significantly mitigate the PKI vulnerabilities.

DOS attacks targeting a DER control center or DER site can be detected by implementing N-ID1 and N-ID2 based on cyber data-based methods [40], physical data-based methods [86], and hybrid methods [87], [88]. RC1 can be realized by designing a communication-free primary inverter controller. For example, a rule-based fallback control strategy [88] is proposed to enhance the resiliency of the microgrid by managing the state of charge of an ESS in a decentralized manner during communication loss of the ESS smart inverter. To mitigate the intentionally delayed measurements and control commands targeting the secondary controller of inverter, Roig Greidanus et al. [86] propose a prediction policy using the inner control loop dynamics to reconstruct a compensating signal locally. Network forensics methods (NF1 and NF2) should be developed to analyze the incidents and assess the defense methods.

B. Malware Defense (Attacks #2–#6)

M-IP2 is designed to screen new files received and classify the files as malware or goodware (benign files) using a static or dynamic malware analysis in a virtual environment. Static

malware analysis examines the incoming binary files by automated reverse engineering methods without running them. Simple static analysis methods utilize static data, such as file header information, file hash, and URL. For example, a smart inverter with PE Studio communicating with online antivirus scanning servers (e.g., VirusTotal) enables to detect known malware files using the extracted static data [74]. Recently, a convolutional neural network based malware file detection with deep transfer learning has been proposed for a device-centric smart inverter malware file detection [69]. This method uses two-dimensional grayscale image files converted from binary files and does not require reverse engineering tools, such as the disassembler. Dynamic analysis methods examine the behavior of malicious files by virtually running them (e.g., Cuckoo Sandbox [90]) that requires relatively higher computational resources and memory space, which might be not relevant to the smart inverter device-level solution. Besides, M-IPS requires unpacking and deobfuscation methods [56] if malware files are packed and obfuscated, which, however, has not been studied in DER devices.

M-IDs are designed to detect malware running in the smart inverter. M-ID1 is designed to detect general malware without considering the types of malware. In [91], ML classifiers are trained and validated by data acquired from hardware performance counters (HPCs). A side-channel malware detection method that utilizes CPU power consumption data [92] is another example of M-ID1. M-ID2 detects a hidden backdoor. As an example, a universal firmware vulnerability observer (UFO) has been used to detect for verifying firmware security and discovering hidden backdoor in an IoT device [93]. M-ID3 and M-ID4 are methods that detect DER botnet devices (e.g., [94]) and DER worm devices communicating with the smart inverter, respectively. MR1 refers to a fast recovery strategy for a malware-infected smart inverter. Continella et al. [95] monitor the filesystem activity over time to compare with a golden image. If this comparison fails (e.g., ransomware executable file injection), a rollback process is promptly initiated. Specifically, MR2 is designed for a fast ransomware recovery strategy. For example, a key backup or discovery method can be utilized to recover ransomware encryptions [96]. CRCs, CRC2–CRC4, are necessary to mitigate the impacts of malware-infected smart inverters. MF is a method of analyzing suspicious or malware-infected smart inverters to learn evolving malware attacks and improve malware defense. As an example, a device-level memory forensics method has been proposed to analyze memory data extracted from a smart inverter [97]. More practical study on CRCs and MF methods is urgently required.

C. HTR Defense (Attack #7)

HT-IP includes the methods of designing and testing ICs and PCBs used in the smart inverter against HTRs. For instance, asset-based structural checking tools can be used to detect malicious insertions in an IC [98]. Assets indicating the roles/contributions will be assigned to all port signals of each module and automatically filtered to all internal signals through the structural checking algorithm. The resulting asset pattern consisting of all assets along each signal path will be analyzed for security evaluation. To protect PCBs from the PCB trojan, an obfuscation-based framework has been proposed [99]. The approach is to use a permutation block that hides the interchip connections between chips on the PCB and is controlled by a key, which allows the correction connections between chips. If the key is not matched, the connections are incorrectly permuted, and the PCB device fails to operate. Besides, an on-chip magnetic probes-inserted PCB design method has been proposed to either prevent the insertion of HTRs or detect them at early stages [100]. The magnetic proves are designed to capture the electromagnetic signature of ICs integrated into the PCB by fully utilizing the remaining metal and polysilicon layers as internal magnetic probes and, in the meantime, deprive the attackers of layout resources to route HTRs.

HT-ID aims to detect hidden HTRs, which were not detected by the HT-IPS. Side-channel analysis-based HTR detection explores changes in its physical parameters (e.g., time [101], power, and electromagnetic radiation). However, this method will have relatively high false alarm rates when detecting small HTR due to the silicon variation and noise. Once the HTR is implemented in the smart inverter, it is not easy to fully recover it without hardware replacement. Thereover, HTR requires a mitigation method against the HTR, which has not been studied yet in DER devices. HTF needs to be developed by using a combination of the state-of-the-art (SOA) HTR testing and detection methods.

D. Controller-Firmware Attack Defense (Attacks #8–10)

CF-IP proactively detects and prevents malicious controller-firmware update, consequently compromising the control algorithm codes, control setting parameters, and controller input data. An example is a blockchain-based firmware patching for a smart inverter [38] with continuous authentication, integrity, and authorization process during the firmware update and the results are stored in the ledger as security logs. Another example is a controller digital twin method, which exams a new version of controller firmware in a twin controller, while the current version of controller firmware still runs in the main controller [39]. CF-IDs are designed to detect malicious controller firmware running in the controller. An example detection method for CF-ID1 and CF-ID2 is an embedded system-tailored HPC technique combined with ML classifiers using real-time features generated by the custom-made HPC [102]. The malicious control algorithm locking and unlocking the inverter every 10 s and modified MPPT setting parameters of a solar microinverter are detected by the MLs. A Kalman filter-based anomaly detection method that can detect falsified inverter sensor data [77] is an example of CF-ID3. CFR demands fast uptime and/or fast CFP methods [39]. The digital twin architecture can also be used to reduce the firmware uptime. Once the operating controller-firmware malfunction event is detected, the standby digital twin controller automatically takes over the primary work of the inverter controller. Another example is an automatic firmware rollback and

patching process through the blockchain-enabled security module [38]. FF methods should be developed, including controller memory forensics.

E. MITM Attacks Defense (Attacks #11 and 12)

CC-IP proactively detects malicious control commands once they are transmitted to the smart inverter. In [45], incoming setpoints are autonomously examined using the knowledge-based self-security technique with reference models and only the safe setpoints are engaged to the inverter's local controller. Meanwhile, a blockchain-based MITM attack detection method is implemented in a solar inverter system by tracking the integrity of the control commands [103]. CC-ID is designed to postdetect a malicious control command after it changes the smart inverter control. Inverter behavior-based anomaly detection methods can be used [45]. In addition, RC2 in the inverter can promptly recover the inverter status from the impact of the malicious control commands.

EM-IPs are considered to prevent and proactively detect external measurement spoofing attacks. EM-IP1 is designed to prevent grid data spoofing attacks. For example, a mathematical hypotheses test [104] is devised to detect a GPS-based grid data spoofing attack that alters a time synchronization of phasor readings leading to affect grid operations as an example of EM-IP1. EM-IP2 is considered to prevent local sensor data spoofing threats. Predefined private (secret) digital watermarking signals in the inverter can distinguish between standard measurement data and spoof data of the grid, local sensors, or sharing data of inverters [105]. EM-IDs detect falsified external measurement spoofing attack by checking inverter status. A data-driven method has been applied to design EM-ID1 and EM-ID2 [41]. Examples of RC against the successful external measurement (RC3 and RC4) can be found in [44] and [106].

F. PE Hardware Attacks Defense (Attacks #13–15)

PE-IP1 recommends appropriate shielding around the PEs' components in the smart inverter against electromagnetic signals. In addition, PE-IP2 recommends preventing physical access and PE-IP3 checks PE hardware layer authenticity when initiating the smart inverter operation (e.g., PCB authentication using *RC* filters [107]). As the PE-IP methods for smart inverters have not been found yet, further studies are necessary. PE-ID1 and PE-ID2 are designed to detect the hall sensor spoofing attack and the side-channel noise injection attack. For example, a Kalman filter-based RC scheme has been proposed to detect and mitigate the side-channel noise injection attack [82]. PE-ID3 provides a comprehensive diagnosis against attacks. A remarkable example method distinguishing between cyberattacks and PE hardware faults can be found in [84], which can further provide designing PEF. However, Fallah et al. [108] assume that firmware is secure and malware cases are not considered. RC8 might be designed by existing fault-tolerant control [108]. Therefore, more research efforts are required to address the hardware layer security for smart inverters.

V. Conclusion

This article discusses an overview of designing cyber-resilient smart inverters based on the comprehensive review of the potential vulnerabilities and challenges of the current best practices and recommendations. Furthermore, practical cyberattacks on the current smart inverters incorporating the current recommendations are introduced. Finally, we propose a smart inverter security and resilience framework and corresponding available defense methods and remaining challenges for developing a next-generation cyber-secure smart inverter security and resilience by design.

The uniqueness of smart inverter security is explained by three security-sensitive layers (network layer, control layer, and PE hardware layer) and the defined attack models considering each layer and their interdependence in the expansion of attack surface environment comparing with other smart grid devices. For example, IoT security and DER device security certification programs mainly focus on a network layer security, while the existing PEs security mainly focus on control layer and PE hardware layer security without detailed attack vectors and cyber dependence. Therefore, the cyber-physical system (CPS) aspect of the system is also considered as the smart inverter that consists of cyber/network layer, control layer, and PE hardware layer and the attack models and corresponding defense methods consider each layer and the interdependence of the layers.

Although the proposed defense strategies for the new security and resilience framework are for new smart inverters to be installed in the near future, legacy smart inverters can adopt available recommended security features through firmware updates (e.g., replacing current cryptography algorithms with the PQC algorithms). Meanwhile, attaching security modules [74], [109] will be an option for the legacy inverters that have no/limited security features. In addition to developing smart inverter security penetration testing methods, it is also noted that the timeliness of FLISR for smart inverters should be defined to evaluate the detection and resilience defense strategies.

Appendix

A criticality assessment of the remaining vulnerabilities, as listed in Table I, is shown in Table IV. This assessment is grounded in MITRE's common attack pattern enumeration and classification (CAPEC) List Ver. 3.9 [110], which offers a comprehensive collection of attack patterns linked to corresponding system vulnerabilities. attackers could disrupt. The criticality score (C) is computed as follows [111]:

$$C \approx \frac{S}{K} \cdot L \tag{1}$$

where S is the severity level of a vulnerability, L is the likelihood of an attack, and K denotes the necessary skill level required for an attack. Each factor is rated and assigned a score of Very High (8), High (4), Medium (2), or Low (1). When multiple rates are presented for a factor, their average rate is computed and, subsequently, taken into consideration to calculate the above expression. The criticality rating for V9–V13 was found to be higher than that of other vulnerabilities. Consequently, this could

TABLE IV
CRITICALITY ASSESSMENT FOR CORRESPONDING VULNERABILITIES

Vulnerability List	Related CAPEC List (Ver. 3.9)	Severity Level of Vulnerability (*S*)	Likelihood of Attack Level (*L*)	Required Attack Skill Level (*K*)	Final Criticality Rating (*C*)
V1. PKI vulnerability in TLS [53]	CAPEC-459: Creating a Rogue Certification Authority Certificate	Very High (8)	Medium (4)	High (6) High (6) Medium (4)	6.00
V2. Password vulnerability in web portal	CAPEC-560: Use of Known Domain Credentials	High (6)	High (6)	Low (2)	18.00
V3. Authorized network masquerading [55]	CAPEC-697: DHCP Spoofing	High (6)	Low (2)	Medium (4)	3.00
V4. Advanced unpacking tools [56]	CAPEC-189: Black Box Reverse Engineering	Low (2)	Medium (4)	Very High (8)	1.00
V5. U-Boot loader vulnerabilities [57]	CAPEC-532: Altered Installed BIOS	High (6)	Low (2)	High (6)	2.00
V6. Spoofed code-signing certificate [58] and Vendor's code-signing system vulnerability [59]	CAPEC-68: Subvert Code-signing Facilities	Very High (8)	Low (2)	High (6)	2.67
V7. Disabling remote patching function by malware	CAPEC-669: Alteration of a Software Update	High (6)	Medium (4)	High (6)	4.00
V8. TPM vulnerability [60]	CAPEC-390: Bypassing Physical Security	High (6)	High (6)	High (6)	6.00
V9. IP masquerading [55]	CAPEC-4: Using Alternative IP Address Encodings	High (6)	Medium (4)	Low (2)	12.00
V10. MFA prompt bombing [61]	CAPEC-600: Credential Stuffing	High (6)	High (6)	Low (2)	18.00
V11. Insider [62]	CAPEC-122: Privilege Abuse	Medium (4)	High (6)	Low (2)	12.00
V12. Local network vulnerability and device access control vulnerabilities	CAPEC-180: Exploiting Incorrectly Configured Access Control Security Levels	Medium (4)	High (6)	Low (2)	12.00
V13. Long recovery time and stolen confidential data [63]	CAPEC-37: Retrieve Embedded Sensitive Data	Very High (8)	High (6)	Medium (4)	12.00
V14. Reactivating debugging interface [64]	CAPEC-702: Exploiting Incorrect Chaining or Granularity of Hardware Debug Components	Medium (4)	Low (2)	Medium (4) Medium (4)	2.00
V15. Side-channel attacks and advanced hardware trojan [65]	CAPEC-624: Hardware Fault Injection	High (6)	Low (2)	High (6)	2.00

make them more attractive to potential attacks on the smart inverter system.

REFERENCES

[1] B. Kroposki et al., "Achieving a 100% renewable grid: Operating electric power systems with extremely high levels of variable renewable energy," *IEEE Power Energy Mag.*, vol. 15, no. 2, pp. 61–73, Mar./Apr. 2017.

[2] S. K. Mazumder et al., "A review of current research trends in power-electronic innovations in cyber–physical systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5146–5163, Oct. 2021.

[3] U.S. Department of Energy-SETO, "Solar futures study," Tech. Rep. GO-102021-5621, Sep. 2021.

[4] Q. Hou, E. Du, N. Zhang, and C. Kang, "Impact of high renewable penetration on the power system operation mode: A data-driven approach," *IEEE Trans. Power Syst.*, vol. 35, no. 1, pp. 731–741, Jan. 2020.

[5] *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources With Associated Electric Power Systems Interfaces*, IEEE Standard 1547-2018, pp. 1–138, Apr. 6, 2018.

[6] *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources With Associated Electric Power Systems Interfaces—Amendment 1: To Provide More Flexibility for Adoption of Abnormal Operating Performance Category III*, IEEE Standard 1547a-2020, pp. 1–16, Apr. 15, 2020.

[7] Y. Xue et al., "On a future for smart inverters with integrated system functions," in *Proc. IEEE 9th Int. Symp. Power Electron. Distrib. Gener. Syst.*, 2018, pp. 1–8.

[8] C. Lai et al., "Cyber security primer for DER vendors, aggregators, and grid operators," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND-2017-13113, Nov. 2017.

[9] B. Ahn, T. Kim, J. Choi, S.-W. Park, K. Park, and D. Won, "A cyber kill chain model for distributed energy resources (DER) aggregation systems," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf.*, 2021, pp. 1–5.

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

[11] CISA, "CISA cybersecurity awareness program small business resources." [Online]. Available: https://www.cisa.gov/publication/cisa-cybersecurity-awareness-program-small-business-resources

[12] K. Park et al., "An advanced persistent threat (APT)-style cyberattack testbed for distributed energy resources (DER)," in *Proc. IEEE Des. Methodol. Conf.*, 2021, pp. 1–5.

[13] E-ISAC, "Analysis of the cyber attack on the Ukrainian power grid: Defense use case," Mar. 2016.

[14] P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber ware," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[15] Trellix, "What is stuxnet?." Accessed: Feb. 1, 2023. [Online]. Available: https://www.trellix.com/en-us/security-awareness/ransomware/what-is-stuxnet.html

[16] S. Lyngaas, "Utah renewables company was hit by rare cyberattack in march," CYBERSCOOP, Oct. 2019. [Online]. Available: https://www.cyberscoop.com/spower-power-grid-cyberattack-foia/

[17] Catherine Stupp, "European wind-energy sector hit in wave of hacks," *The Wall Street J*, Apr. 25, 2022. [Online]. Available: https://www.wsj.com/articles/European-wind-energy-sector-hit-in-wave-of-hacks-11650879000

[18] Eclypsium, "Conti targets critical firmware," Jun. 2022. [Online]. Available: https://eclypsium.com/2022/06/02/conti-targets-critical-firmware/

[19] M. Raggi and S. Scenarelli, "Rising tide: Chasing the currents of espionage in the South China sea," Proofpoint, Aug. 2022. [Online]. Available: https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-China-sea

[20] IEC 62351-12, Apr. 2016. [Online]. Available: https://webstore.iec.ch/publication/24474

[21] J. Johnson, "Roadmap for photovoltaic cyber security," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2017-13262, Dec. 2017.

[22] A. Sanghvi et al., "Roadmap for wind cybersecurity," U.S. Dept. Energy, Washington DC, USA, Tech. Rep. DOE/GO-102020-8441, Jul. 2020.

[23] 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-Phys. Syst., Theory Appl.*, vol. 5, no. 3, pp. 274–282, Sep. 2020.

[24] J. Obert et al., "Recommendations for trust and encryption in DER interoperability standards," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2019-1490, Feb. 2019.

[25] I. Onunkwo, "Recommendations for data-in-transit requirements for securing DER communications," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2020-12704, Nov. 2020.

[26] J. Johnson, "Recommendations for distributed energy resource access control," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2021-0977, Jan. 2021.

[27] J. Johnson and I. Hanke, "Recommendations for distributed energy resource patching," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2021-11150, Sep. 2021.

[28] J. Johnson, I. Onunkwo, D. Saleem, W. Hupp, J. Peterson, and R. Cryar, "Distributed energy resource cybersecurity standards development—Final project report," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2022-1118, Jan. 2022.

[29] D. Saleem and C. Carter, "Certification procedures for data and communications security of distributed energy resources," Nat. Renewable Energy Lab., Golden, CO, USA, Tech. Rep. NREL/TP-5R00-73628, Jul. 2019.

[30] UL Solutions, "UL and NREL announce cybersecurity testing recommendations for distributed energy resources and inverter based resources," Mar. 2022. [Online]. Available: https://www.ul.com/news/ul-and-nrel-announce-cybersecurity-testing-recommendations-distributed-energy-resources-and

[31] California Rule 21, Jul. 21, 2017. [Online]. Available: https://www.cpuc.ca.gov/Rule21/

[32] SunSpec Certification. Accessed: Feb. 1, 2023. [Online]. Available: https://sunspec.org/certification/

[33] "IEEE guide for cybersecurity of distributed energy resources interconnected with electric power systems," in IEEE Std 1547.3-2023 (Revision of IEEE Std 1547.3-2007), pp. 1–183, Dec. 2023.

[34] D. J. Sebastian and A. Han, "Exploring emerging cybersecurity risks from network-connected der devices," in *Proc. IEEE North Amer. Power Symp.*, 2017, pp. 1–6.

[35] T. S. Ustun, "Cybersecurity vulnerabilities of smart inverters and their impacts on power system operation," in *Proc. IEEE Int. Conf. Power Electron., Drives, Energy Syst.*, 2019, pp. 1–4.

[36] S. M. S. Hussain and T. S. Ustun, "Smart inverter communication model and impact of cybersecurity attack," in *Proc. IEEE Int. Conf. Power Electron., Drives Energy Syst.*, 2020, pp. 1–5.

[37] F. Zhang and Q. Li, "Security vulnerability and patch management in electric utilities: A data-driven analysis," in *Proc. 1st Workshop Radical Experiential Secur.*, 2018, pp. 65–68.

[38] G. Bere, B. Ahn, J. J. Ochoa, T. Kim, A. A. Hadi, and J. Choi, "Blockchain-based firmware security check and recovery for smart inverters," in *Proc. IEEE Appl. Power Electron. Conf. Expo.*, 2021, pp. 675–679.

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

[40] 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 *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf.*, 2020, pp. 1–5.

[41] 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 *Proc. IEEE Energy Convers. Congr. Expo.*, 2020, pp. 431–436.

[42] Z. Zhang, M. Easley, M. Hosseinzadehtaher, G. Amariucai, M. B. Shadmand, and H. Abu-Rub, "An observer based intrusion detection framework for smart inverters at the grid-edge," in *Proc. IEEE Energy Convers. Congr. Expo.*, 2020, pp. 1957–1962.

[43] J. Ramos-Ruiz et al., "An active detection scheme for cyber attacks on grid-tied PV systems," in *Proc. IEEE CyberPELS*, 2020, pp. 1–6.

[44] S. Sahoo, T. Dragičević, Y. Yang, and F. Blaabjerg, "Adaptive resilient operation of cooperative grid-forming converters under cyber attacks," in *Proc. IEEE CyberPELS*, 2020, pp. 1–5.

[45] M. Gursoy and B. Mirafzal, "Self-security for grid-interactive smart inverters using steady-state reference model," in *Proc. IEEE 22nd Workshop Control Modelling Power Electron.*, 2021, pp. 1–5.

[46] Y. Li and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Trans. Power Electron.*, vol. 38, no. 2, pp. 2364–2383, Feb. 2023.

[47] Kitu Syst. Accessed: Jan. 20, 2023. [Online]. Available: https://www.kitu.io/

[48] SMA inverter. Accessed: Jan. 20, 2023. [Online]. Available: https://www.sma-America.com/products/solarinverters

[49] EPRI, "EPRI security architecture for the distributed energy resources integration network," Oct. 2019. [Online]. Available: https://sunspec.org/wp-content/uploads/2020/01/EPRI-Security-Architecture-for-the-Distributed-Energy-Resources-Integration-Network.pdf

[50] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," NIST Special Publication 800-94, Feb. 2007. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf

[51] W. C. Barker, W. Fisher, K. Scarfone, and M. Souppaya, "Ransomware risk management: A cybersecurity framework profile," NISTIR 8374, Feb. 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf

[52] C. Skouloudi, A. Malatras, R. Naydenov, and G. Dede, "Guidelines for securing the Internet of Things," ENISA, Nov. 2020. [Online]. Available: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[53] T. Dai, H. Shulman, and M. Waidner, "Off-path attacks against PKI," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2018, pp. 2213–2215.

[54] M. K. Ferst, H. F. M. de Figueiredo, and G. W. Denardin, "Connection time in modbus/TLS for secure communications on photovoltaic systems," in *Proc. IEEE 15th Braz. Power Electron. Conf., 5th IEEE Southern Power Electron. Conf.*, 2019, pp. 1–6.

[55] VMWare, "The four barriers to micro-segmentation," White Paper, Mar. 2020. [Online]. Available: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-wp-four-barrs-micro-segmntatn-uslet-Final.pdf

[56] M. Bat-Erdene, T. Kim, H. Park, and H. Lee, "Packer detection for multilayer executables using entropy analysis," *Entropy*, vol. 19, Mar. 2017, Art. no. 125.

[57] I. Arghire, "Critical U-boot vulnerability allows rooting of embedded systems," Security Week, [Online]. Available: https://www.securityweek.com/critical-u-boot-vulnerability-allows-rooting-embedded-systems

[58] P. Arntz, "Stolen Nvidia certificates used to sign malware—Here's what to do," Malwarebytes, Mar. 2022. [Online]. Available: https://www.malwarebytes.com/blog/news/2022/03/stolen-nvidia-certificates-used-to-sign-malware-heres-what-to-do

[59] SolarWinds Supply Chain Attack, Nov. 30, 2022. [Online]. Available: https://www.fireeye.com/blog/threat-research/2021/01/remediation-and-hardening-strategies-for-microsoft-365-to-defend-against-unc2452.html

[60] D. Moghimi, B. Sunar, T. Eisenbarth, and N. Heninger, "TPM-fail: TPM meets timing and lattice attacks," in *Proc. 29th USENIX Secur. Symp.*, 2020, pp. 2057–2073.

[61] "Lapsus$ and SolarWinds hackers both use the same old trick to bypass MFA," Mar. 29, 2022. [Online]. Available: https://arstechnica.com/information-technology/2022/03/lapsus-and-solar-winds-hackers-both-use-the-same-old-trick-to-bypass-mfa/

[62] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, and Y. Xiang, "Detecting and preventing cyber insider threats: A survey," *IEEE Commun. Surv. Tut.*, vol. 20, no. 2, pp. 1397–1417, Apr./Jun. 2018.

[63] Y. Su, B. Ahn, S. R. B. Alvee, T. Kim, J. Choi, and S. C. Smith, "Ransomware security threat modeling for photovoltaic systems," in *Proc. IEEE 6th Workshop Electron. Grid*, 2021, pp. 1–5.

[64] S. Quinn and S. Povolny, "A door isn't a door when it's ajar—Part I," Trellix, Aug. 2022. [Online]. Available: https://www.trellix.com/en-us/about/newsroom/stories/research/a-door-is-not-a-door-when-its-jar.html

[65] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware trojan attacks: Threat analysis and countermeasures," *Proc. IEEE*, vol. 102, no. 8, pp. 1229–1247, Aug. 2014.

[66] J. Ahn et al., "Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (PQC) and quantum key distribution (QKD)," *Energies*, vol. 15, Jan. 2022, Art. no. 714.

[67] S. Ahmad et al., "Blockchain-integrated resilient distributed energy resources management system," in *Proc. IEEE SmartGridComm*, 2022, pp. 59–64.

[68] J. Choi, D. Narayanasamy, B. Ahn, S. Ahmad, J. Zeng, 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 *Proc. IEEE Int. Symp. Power Electron. Distrib. Gener. Syst.*, 2021, pp. 1–5.

[69] S. Alvee, B. Ahn, S. Ahmad, K. Kim, T. Kim, and J. Zeng, "Device-centric firmware malware detection for smart inverters using deep transfer learning," in *Proc. IEEE Des. Methodol. Power Electron.*, 2022, pp. 1–5.

[70] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. 27th USENIX Secur. Symp.*, 2018, pp. 15–32.

[71] P. Eder-Neuhauser, T. Zseby, and J. Fabini, "Malware propagation in smart grid networks: Metrics, simulation and comparison of three malware types," *J. Comput. Virol. Hacking Techn.*, vol. 15, pp. 109–125, 2019.

[72] "Super micro spy chip," Feb. 12, 2021. [Online]. Available: https://9to5mac.com/2021/02/12/super-micro-spy-chip-story/

[73] S. Ghosh, A. Basak, and S. Bhunia, "How secure are printed circuit boards against trojan attacks?," *IEEE Des. Test*, vol. 32, no. 2, pp. 7–16, Apr. 2015.

[74] B. Ahn, G. Bere, S. Ahmad, J. Choi, T. Kim, and S.-W. Park, "Blockchain-enabled security module for transforming conventional inverters toward firmware security-enhanced smart inverters," in *Proc. IEEE Energy Convers. Congr. Expo.*, 2021, pp. 1307–1312.

[75] 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. 29775–29818, 2021.

[76] The U.S. Department of Energy, "Cybersecurity considerations for distributed energy resources on the U.S. electric grid," Washington, DC, USA, Oct. 2022.

[77] J. Zhang and J. Ye, "Cyber-attack detection for active neutral point clamped (ANPC) photovoltaic (PV) converter using Kalman filter," in *Proc. IEEE Appl. Power Electron. Conf. Expo.*, 2022, pp. 1939–1944.

[78] J. Choi, B. Ahn, S. Pedavalli, S. Ahmad, A. Villasenor, and T. Kim, "Secure firmware update and device authentication for smart inverter using blockchain and physically unclonable function (PUF)-embedded security module," in *Proc. IEEE 6th Workshop Electron. Grid*, 2021, pp. 1–4.

[79] J. Ye et al., "A review of cyber-physical security for photovoltaic systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 4, pp. 4879–4901, Aug. 2022.

[80] A. Barua and M. A. Al Farugue, "Hall spoofing: A non-invasive dos attack on grid-tied solar inverter," in *Proc. 29th USENIX Secur. Symp.*, 2020, pp. 1273–1290.

[81] J. Selvaraj, "Intentional electromagnetic interference attack on sensors and actuators," Ph.D. dissertation, Dept. Elect. Comput. Eng., Iowa State Univ., Ames, IA, USA, 2018.

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

[83] S. K. Mazumder, M. D. R. Greidanus, J. Liu, and H. A. Mantooth, "Vulnerability of a VOC-based inverter due to noise injection and its mitigation," *IEEE Trans. Power Electron.*, vol. 38, no. 2, pp. 1445–1450, Feb. 2023.

[84] K. Gupta, S. Sahoo, R. Mohanty, B. Ketan Panigrahi, and F. Blaabjerg, "Distinguishing between cyber attacks and faults in power electronic systems—A noninvasive approach," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 11, no. 2, pp. 1578–1588, Apr. 2023.

[85] NIST Cybersecurity Framework (Ver. 1.1). [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[86] M. D. Roig Greidanus, S. Sahoo, S. Mazumder, and F. Blaabjerg, "Novel control solutions for DoS attack delay mitigation in grid-connected and standalone inverters," in *Proc. IEEE 12th Int. Symp. Power Electron. Distrib. Gener. Syst.*, 2021, pp. 1–7.

[87] C. C. Sun, R. Zhu, and C. C. Liu, "Cyber attack and defense for smart inverters in a distribution system," in *Proc. CIGRE Study Committee D2 Colloq.*, 2019, Paper 1824577.

[88] A. Chavez et al., "Hybrid intrusion detection system design for distributed energy resource systems," in *Proc. IEEE CyberPELS*, 2019, pp. 1–6.

[89] M. Chlela, D. Mascarella, G. Joós, and M. Kassouf, "Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4702–4711, Sep. 2018.

[90] Cuckoo Sandbox, Jun. 23, 2023. [Online]. Available: https://www.varonis.com/blog/cuckoo-sandbox

[91] K. I. Gubbi, H. Wang, H. Sayadi, and H. Homayoun, "Machine learning based malware detection for secure smart grids," in *Proc. 11th Int. Conf. Renewable Energy Res. Appl.*, 2022, pp. 330–334.

[92] J. H. Jimenez and K. Goseva-Popstojanova, "Malware detection using power consumption and network traffic data," in *Proc. 2nd Int. Conf. Data Intell. Secur.*, 2019, pp. 53–59.

[93] C.-W. Tien, T.-T. Tsai, I.-Y. Chen, and S.-Y. Kuo, "UFO—Hidden backdoor discovery and security verification in IoT device firmware," in *Proc. IEEE Int. Symp. Softw. Rel. Eng. Workshops*, 2018, pp. 18–23.

[94] C. Dietz, G. Dreo, A. Sperotto, and A. Pras, "Towards adversarial resilience in proactive detection of botnet domain names by using MTD," in *Proc. IEEE/IFIP NOMS Netw. Oper. Manage. Symp.*, 2020, pp. 1–5.

[95] A. Continella et al., "ShieldFS: A self-healing, ransomware-aware filesystem," in *Proc. 32nd Annu. Conf. Comput. Secur. Appl.*, 2016, pp. 336–347.

[96] K. Lee, K. Yim, and J. Seo, "Ransomware prevention technique using key backup," *Concurrency Comput., Pract. Experience*, vol. 30, no. 3, 2018, Art. no. e4337.

[97] A. M. Jenkins, B. Ahn, A. Akash, and T. Kim, "Device-centric ransomware detection using machine learning-based memory forensics for smart inverters," in *Proc. 8th Annu. Ind. Control System Secur. Workshop*, 2022, pp. 1–7.

[98] T. Le, L. Weaver, J. Di, S. Zhang, and Y. Jin, "Hardware trojan detection and functionality determination for soft IPs," in *Proc. IEEE 3rd Int. Verification Secur. Workshop*, 2018, pp. 56–61.

[99] Z. Guo, J. Di, M. M. Tehranipoor, and D. Forte, "Obfuscation-based protection framework against printed circuit boards unauthorized operation and reverse engineering," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 22, no. 3, Jul. 2017, Art. no. 54.

[100] T. M. Supon and R. Rashidzadeh, "On-chip magnetic probes for hardware trojan prevention and detection," *IEEE Trans. Electromagn. Compat.*, vol. 63, no. 2, pp. 353–364, Apr. 2021.

[101] V. Venugopalan, C. D. Patterson, and D. M. Shila, "Detecting and thwarting hardware trojan attacks in cyber-physical systems," in *Proc. IEEE Conf. Commun. Netw. Secur.*, 2016, pp. 421–425.

[102] A. P. Kuruvila, L. Zografopoulos, K. Basu, and C. Konstantinou, "Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids," *Int. J. Elect. Power Energy Syst.*, vol. 132, Nov. 2021, Art. no. 107150.

[103] J. Choi, B. Ahn, G. Bere, S. Ahmad, H. A. Mantooth, and T. Kim, "Blockchain-based man-in-the-middle (MITM) attack detection for photovoltaic systems," in *Proc. IEEE Des. Methodol. Conf.*, 2021, pp. 1–6.

[104] P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore, and R. S. Blum, "GPS spoofing attack characterization and detection in smart grids," in *Proc. IEEE Conf. Commun. Netw. Secur.*, 2016, pp. 391–395.

[105] H. Ibrahim et al., "An active detection scheme for sensor spoofing in grid-tied PV systems," in *Proc. IEEE Energy Convers. Congr. Expo.*, 2021, pp. 1433–1439.

[106] A. Abbaspour, A. Sargolzaei, P. Forouzannezhad, K. K. Yen, and A. I. Sarwat, "Resilient control design for load frequency control system under false data injection attacks," *IEEE Trans. Ind. Electron.*, vol. 67, no. 9, pp. 7951–7962, Sep. 2020.

[107] S. Lee, M.-K. Oh, Y. Kang, and D. Choi, "Design of resistor-capacitor physically unclonable function for resource-constrained IoT devices," *Sensors*, vol. 20, no. 2, Jan. 2020, Art. no. 404.

[108] F. Fallah, A. Ramezani, and A. Mehrizi-Sani, "Integrated fault diagnosis and control design for DER inverters using machine learning methods," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2022, pp. 1–5.

[109] W. Hupp, A. Hasandka, R. S. de Carvalho, and D. Saleem, "ModuleOT: A hardware security module for operational technology," in *Proc. IEEE Texas Power Energy Conf.*, 2020, pp. 1–6.

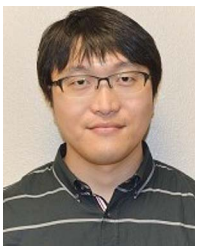
[110] CAPEC. Accessed: Aug. 27, 2023. [Online]. Available: https://capec.mitre.org/index.html

[111] B. Ahn, A. Jenkins, T. Kim, J. Zeng, L. McLauchlan, and S. Park, "Exploring ransomware attacks on smart inverters," in *Proc. IEEE Energy Convers. Congr. Expo.*, Nashville, TN, USA, 2023, pp. 1567–1573.

BoHyun Ahn (Graduate Student Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Minnesota State University, Mankato, Mankato, MN, USA, in 2016 and 2018, respectively. He is currently working toward the Ph.D. degree in electrical engineering with Texas A&M University-Kingsville, Kingsville, TX, USA.

His current research interests include cyber-secure smart inverter, penetration testing, blockchain-based security, firmware security, and malware defense.

Mr. Ahn was a recipient of first place in the 2022 IEEE ECCE student demo project software competition.



Taesic Kim (Senior Member, IEEE) received the B.S. degree in electronics engineering from Changwon National University, Changwon, South Korea, in 2008, and the M.S. and Ph.D. degrees in electrical engineering and computer engineering from the University of Nebraska–Lincoln, Lincoln, NE, USA, in 2012 and 2015, respectively.

In 2009, he was with New and Renewable Energy Research Group, Korea Electrotechnology Research Institute, South Korea. He was also with Mitsubishi Electric Research Laboratories, Cambridge, MA, USA, in 2013. He is currently an Associate Professor with the Department of Electrical Engineering and Computer Science, Texas A&M University–Kingsville, Kingsville, TX, USA. His research interests now cover broad areas of cyber-physical power and energy systems, including cyber-physical system security, power electronics and cyber-resilient power systems, quantum machine learning and optimization, and blockchain.

Dr. Kim 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.

Seerin Ahmad (Graduate Student Member, IEEE) received the B.S. degree from Aligarh Muslim University, Aligarh, India, in 2017, and the M.S. degree from the Budapest University of Technology and Economics, Budapest, Hungary, in 2019, both in electrical engineering. He is currently working toward the Ph.D. degree in electrical engineering with Texas A&M University-Kingsville, Kingsville, TX, USA.

His research interests include cyber-resilient power systems, distributed energy resource management system, power electronics, and cybersecurity.

Sudip Kumar Mazumder (Fellow, IEEE) received the Ph.D. degree in electrical and computer engineering from Virginia Tech, Blacksburg, VA, USA, in 2001.

He is an UIC Distinguished Professor with the Department of Electrical and Computer Engineering, University of Illinois, Chicago, IL, USA. He has also been the President of NextWatt LLC, Kanhangad, Kerala, since 2008.

Dr. Mazumder was the recipient of the 2023 IEEE Power and Energy Society's Ramakumar Family Renewable Energy Excellence Award, several IEEE awards/honors, including IEEE Transactions on Power Electronics Prize Paper Awards in 2002 and 2022 and Highlighted Papers in 2018, 2022, and 2023, Featured Article for IEEE Transactions on Biomedical Engineering in 2023, IEEE Conference Best Paper Award in 2013, and IEEE International Future Energy Challenge Award in 2005. He was named a Fellow of the American Association for the Advancement of Science, in 2020, and a Fellow of the Asia-Pacific Artificial Intelligence Association, in 2022. He has been an Editor in Large for IEEE TRANSACTIONS ON POWER ELECTRONICS since 2019 and served as an IEEE Distinguished Lecturer between 2016 and 2019. He has been serving as an Administrative Committee Member for IEEE PELS, since 2015. He has also been serving as a Member-at-Large for IEEE PELS, since 2020. He served as the Chair for the IEEE PELS Technical Committee on Sustainable Energy Systems, from 2015 to 2020. He served as the General Chair for IEEE PEDG Conference in 2023 and serves as the General Co-Chair for IEEE Energy Conversion Congress and Exposition in 2024.

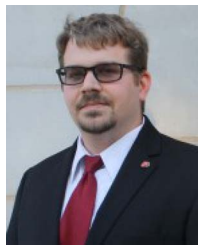
Jay Johnson (Senior Member, IEEE) received the B.S. degree from the University of Missouri-Rolla, Rolla, MO, USA, in 2006, and the M.S. degree from the Georgia Institute of Technology, Atlanta, GA, USA, in 2009, both in mechanical engineering.

He is the Chief Technology Officer with DER Security Corp, a startup company focused on distributed energy resource communications, power operations, and security. His team is building cybersecurity protection, detection, and response technologies for EV chargers, renewable energy installations, and energy storage systems. He was a Distinguished Member of Technical Staff with Sandia National Laboratories, where he led research projects totaling $25M in the areas of power system control, optimization, and security. He has authored more than 150 academic papers, has eight issued patents, and was interviewed for Wired, Forbes, NPR, and several other media outlets on his EV charger cybersecurity research.

H. Alan Mantooth (Fellow, IEEE) received the B.S.E.E. and M.S.E.E. degrees from the University of Arkansas (UA), Fayetteville, AR, USA, in 1985 and 1986, respectively, and the Ph.D. degree from Georgia Tech, Atlanta, GA, USA, in 1990.

He then joined Analogy, a startup company in Oregon. After 8 years with Analogy, he joined the faculty of the Department of Electrical Engineering, University of Arkansas, Fayetteville, AR, USA, where he currently holds the rank of a Distinguished Professor. His research interests now include analog and mixed-signal IC design and CAD, semiconductor device modeling, power electronics, power electronic packaging, and cybersecurity. He helped establish and direct the National Center for Reliable Electric Power Transmission, UA, in 2005. He serves as the Founding Director of the NSF Industry/University Cooperative Research Center on GRid-Connected Advanced Power Electronic Systems and the Deputy Director of the NSF ERC on Power Optimization of Electro-Thermal Systems. He holds the 21st Century Research Leadership Chair in Engineering. He is a past President of the IEEE Power Electronics Society and currently serves as an Editor-in-Chief for the *IEEE Open Journal of Power Electronics*. He is serving as Division II Director-Elect in 2024 and the Director in 2025 and 2026 on the IEEE Board of Directors. He is a member of Tau Beta Pi, Sigma Xi, and Eta Kappa Nu.

Dr. Mantooth is a Registered Professional Engineer in Arkansas.



Chris Farnell (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Arkansas, Fayetteville, AR, USA, in 2020.

He is currently an Assistant Professor with Electrical Engineering and Computer Science Department, University of Arkansas. His research interests include cybersecurity for critical infrastructure, embedded system design, FPGA design, advanced control algorithms, and power electronics. He is currently serving as an Associate Director of the National Center for Reliable Electric Power Transmission, University of Arkansas. This 12 000 ft^2 laboratory provides the equipment, technical staff, and instrumentation to test and evaluate power electronic circuits and systems at realistic industrial and distribution voltage levels up to 6 MVA power ratings. He is the current Chair of the IEEE Ozark Section, treasurer for the newly formed IEEE Computer Society Chapter, the CyberHogs Registered Student Organization faculty mentor, and remains active in K-12 outreach activities.