Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations

Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations

Ioannis Zografopoulos, *Graduate Student Member, IEEE*, Nikos D. Hatziargyriou, *Life Fellow, IEEE*, Charalambos Konstantinou, *Senior Member, IEEE*

***Abstract*—The digitization and decentralization of the electric power grid are key thrusts for an economically and environmentally sustainable future. Towards this goal, distributed energy resources (DER), including rooftop solar panels, battery storage, electric vehicles, etc., are becoming ubiquitous in power systems. Power utilities benefit from DERs as they minimize operational costs; at the same time, DERs grant users and aggregators control over the power they produce and consume. DERs are interconnected, interoperable, and support remotely controllable features, thus, their cybersecurity is of cardinal importance. DER communication dependencies and the diversity of DER architectures widen the threat surface and aggravate the cybersecurity posture of power systems. In this work, we focus on security oversights that reside in the cyber and physical layers of DERs and can jeopardize grid operations. Existing works have underlined the impact of cyberattacks targeting DER assets, however, they either focus on specific system components (e.g., communication protocols), do not consider the mission-critical objectives of DERs, or neglect the adversarial perspective (e.g., adversary/attack models) altogether. To address these omissions, we comprehensively analyze adversarial capabilities and objectives when manipulating DER assets, and then present how protocol and device-level vulnerabilities can materialize into cyberattacks impacting power system operations. Finally, we provide mitigation strategies to thwart adversaries and directions for future DER cybersecurity research.**

***Index Terms*—Cybersecurity, distributed energy resources, attacks, mitigations.**

I. Introduction

In the last decades, electric power systems (EPS) have undergone significant transformations (e.g., decentralized generation, digitization of customer services, smart grid initiatives, etc.) to meet the increasing power demand and provide economically and environmentally friendly energy. Renewable energy resources (RES) harnessing wind, solar, and thermal energy have been used to improve energy efficiency while meeting stringent carbon emission regulations [1]. The shift towards more sustainable grid architectures has also boosted the adoption of distributed energy resources (DER). According to the definition of the North American Electric Reliability Corporation (NERC), DERs are distribution-level resources that produce electricity and are not part of the bulk EPS [2].

DERs can leverage renewable or non-renewable resources. DER devices are classified into different categories based on their operation principles, e.g., generation, energy storage, combination of the two, or controllable loads. Solar panels and wind turbines belong to the generation category [3], batteries and EVs fall into energy storage, combined cooling and heating, and electric water heaters are examples of controllable loads [4], and inverter-based resources (IBR) can be used in both generation and storage scenarios.

The rapid integration of DERs highlights their importance for EPS and the global generation capacity is expected to grow from 132.4 GW in 2017 to 528.4 GW by 2026 [5]. Similar observations can be made for battery energy storage systems (BESS). Namely, in the United States (U.S.), BESS are expected to grow from 1.2 GW in 2020 to nearly 7.5 GW in 2025, while developing into a market of $7.3 billion annually [6]. Strategic placement of DERs, can utilize on-site generation and minimize utility costs by deferring investments for the expansion of the power system network. DER-generated power does not need to be transferred from remote bulk generation facilities, minimizing energy losses and providing economically dispatchable power. DERs could reduce transmission system operator (TSO) ancillary market costs, which increased by almost 70% during the 2020 COVID-19 lockdown [7]. This was due to the stochasticity of real-time power demand and the requirement to maintain frequency stability and energy reserves, mainly relying on the intermittent generation of RES, which created a very competitive power market. DERs can enhance EPS reliability through DER-supported autonomous functions. With higher DER penetration, the consequences of disastrous events could be averted or effectively mitigated [8]. For instance, DERs could alleviate the impacts of extreme weather events similar to the Texas snowstorm in February 2021 [9].

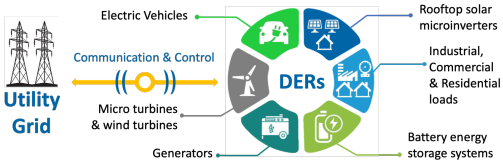

Fig. 1: Utility-to-DER interconnection.

The flexible and autonomous attributes of DERs render them invaluable pillars for the EPS critical infrastructure (CI). Being crucial parts of the EPS, DERs can become prominent cyberattack targets. Attackers could exploit vulnerabilities, i.e., weaknesses in a system that can be leveraged to carry out an attack, to compromise remote communication, gain control of DERs, and propagate attack impacts to the rest of the system. The cybersecurity incident in Utah, U.S. on 5 March 2019 is a prime example of how compromised communications can affect grid services. In this incident, attackers exploited vulnerabilities in security firewall devices to halt communications between system operators and distribution wind and solar utilities [10]. The impact of this denial-of-service (DoS) attack caused loss of visibility of power grid assets and could have caused interruptions of electrical system operations [11]. To overcome cyberattacks comprehensive security investigations should be performed taking into account the *cyber-physical* DER nature.

On the cyber level, protocols facilitate the communication between DERs and utility aggregators for DER monitoring and control purposes (Fig. 1). Information and communica-

tion technologies (ICT) enable communication between DER assets and DER management systems (DERMS). Typically, wired or wireless communication protocols are used, such as the IEEE 1815-Distributed Network Protocol (DNP3), Sunspec Modbus, open automated demand response (OpenADR), and IEEE 2030.5 (Table I). Embedded devices on the DER side handle monitoring and remote DER asset control requests. Insecure remote communication expands the EPS threat surface since adversaries can exploit communication protocol weaknesses to mount attacks, e.g., DoS, man-in-the-middle (MitM), etc. The situation is aggravated by the fact that many of the communication protocols have known vulnerabilities, which if exploited, can compromise system operation by issuing malicious commands to DER end-devices.

On the physical layer, the device-level consists of the embedded architectures (e.g., controllers, gateways, converters, etc.) and their fundamental components (e.g., hardware, firmware, software, etc.) that support DER operations and could constitute another weak link for the system security. Most of these embedded devices are built using commercial off-the-shelf (COTS) components that could suffer from hardware- and software- level vulnerabilities. Apart from the vulnerabilities of COTS and the computational resource constraints of embedded systems (which limits the sophistication of security schemes), their trustworthiness cannot be attested either. The heterogeneity of embedded systems aggravates their security posture and makes verifying the supply-chain trustworthiness often infeasible. Multiple third-party vendors provide intellectual property (IP) blocks which are then integrated by fabrication facilities during manufacturing [12]. Apart from hardware IP blocks, software supply-chain compromises, where threat actors intentionally plant backdoors into software products to weaponize it later is also a major concern [13]. The severe impact of supply-chain attacks was demonstrated during the Solarwinds incident in December 2020, which targeted network management systems around the globe. Namely, $18k$ of the $300k$ Solarwinds customers were running vulnerable versions of the Orion platform, including the U.S. Department of Treasury, U.S. Department of Energy, U.S. Department of Defense, 425 of the U.S. Fortune 500, as well as the cybersecurity firm FireEYE [14]. The severe blow of the Solarwinds supply-chain attack on CI networks forced the White House to issue an executive order instructing the improvement of cybersecurity in all federal government networks [15]. Supply-chain-related dependencies arise as potential threat vectors, i.e., specific paths or methods that can be exploited to compromise a system, especially given the lack of security controls when designing or integrating COTS software or hardware during system design.

Sophisticated cyberattacks targeting CI are gaining popularity given the severe impacts on business operations like the Solarwinds incident and the colonial pipeline ransomware attack which halted the delivery of transport fuel to the Atlantic coast [21]. Furthermore, attacks on public health are rising, such as the attack on the Florida water treatment plant [22], attacks on hospitals during COVID-19 [23], etc. The aforementioned incidents underline that CI protection needs to become the epicenter of cybersecurity research. In Fig. 2, we demonstrate a timeline of cyberattacks targeting the energy and other CI sectors that have been reported in the literature. The rapid penetration of inverter-based DERs has displaced synchronous generation arising concerns about the stability of IBR-dominated systems. Ancillary services, such as synthetic inertia, are crucial to maintaining frequency stability in grid and microgrid architectures composed of non-synchronous DERs [20]. However, from an adversarial perspective, these services can be exploited to destabilize such inertia-less systems, as demonstrated in Fig. 3.

TABLE I: Common DER communication protocols.

Protocol	Description	Std.
IEEE 1815 DNP3	Interoperable communication framework for secure information exchange in industrial systems (e.g., SCADA)	[16]
Sunspec Modbus	Modbus protocol extension for DER parameters (e.g., power, voltage) and ancillary services monitoring and control	[17]
OpenADR	Energy market management standard regulating demand-response via signals to DERs and other controllable devices	[18]
IEEE 2030.5	Smart energy profile application standard and default protocol for DER management	[19]

To combat threats related to DER, existing efforts such as the DER cybersecurity framework (DERCF) by the National Renewable Energy Lab (NREL) [24], and the renewable energy and distributed systems integration (RDSI) program by Sandia National Lab (SNL) [25], place grid security as one of their core initiatives. Cybersecurity endeavors led by academic institutions have also attempted to identify vulnerabilities in DERs, and more specifically inverter-based systems. For instance, [26] and [27] provide a detailed description of the smart inverter operational objectives and ancillary grid support functions. In [27], the authors discuss a variety of cyberattack and potential mitigation strategies. However, the connection between adversarial incentives and the resources necessary to perform such compromises is overlooked. In [28], [29] a comprehensive review of detection and defense methodologies is presented to overcome contingencies in PV systems. However, some of the prescribed defense strategies, e.g., blockchain, neglect the operational technology (OT) constraints and limitations of the underlying field devices.

Research efforts have also identified existing vulnerabilities in communication protocols, used for the orchestration of DER, that can be exploited as threat vectors [30], [31]. The standards defining the security objectives of such protocols are compiled in [32] along with cybersecurity principles that could help overcome communication-related threats. However, the performance overhead, associated with improving the security of such protocols, is not discussed. In [33], the authors investigate the impact of securing the communication infrastructure on the real-time operation of DERs in a network co-simulation environment. Suggestions to overcome protocol cybersecurity limitations and metrics to assess cyberattack impacts are also reported, while simulation tools to measure the efficacy of protocol defenses are delineated in [34].

In this paper, we focus on cyberattacks targeting DER assets on both the *device* and *communication* levels. We discuss cyberattacks targeting the DER devices themselves and their

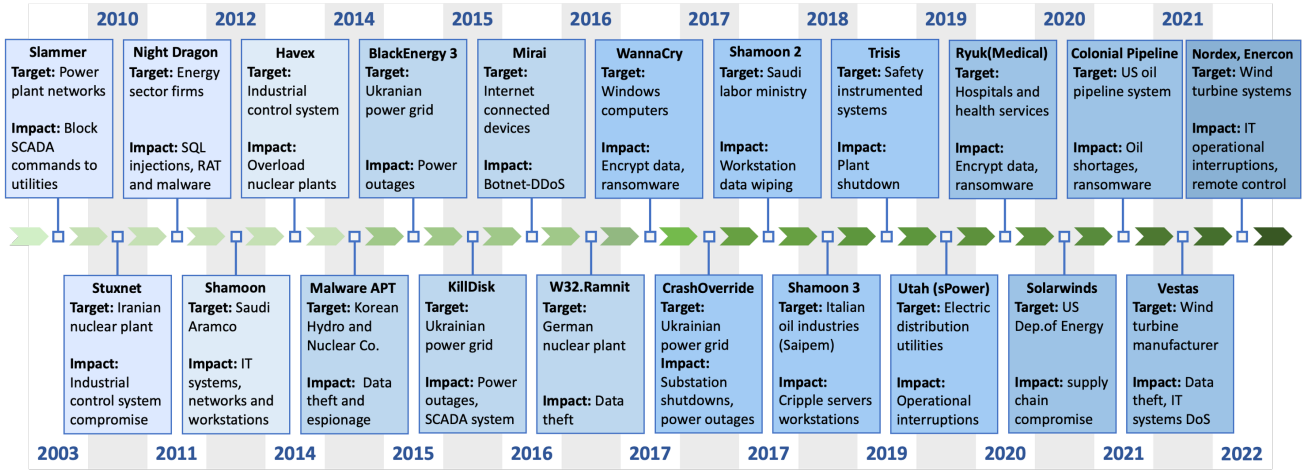

Fig. 2: Timeline of cyberattacks targeting the energy sector and other critical infrastructure sectors.

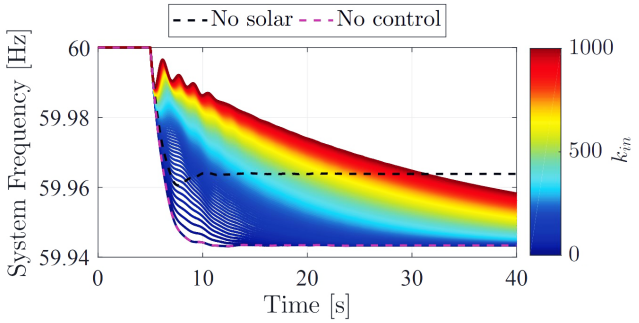

Fig. 3: Impact of synthetic inertia gain (k_{in}) on system frequency response [20].

autonomous capabilities (e.g., defensive islanding) and ancillary services (e.g., voltage/frequency regulation, active/reactive power compensation, etc.). DER security should be viewed holistically and is contingent upon the security posture of the inherent DER device architectures (e.g., vendor-specific), the utilized communication protocols, and control schemes (e.g., user, aggregator, or utility -defined). Comprehensive security solutions should encompass an *adversary viewpoint* capable of not only mitigating previous incidents (as most of the literature does), but proactively defending against "what could happen" scenarios. To bridge this overlooked research gap, we first discuss the motives and resources of adversaries and the crucial components of DER systems before we focus on DER attacks at the *i)* communication protocol and *ii)* device levels. Last, DER protocol- and device- level vulnerabilities, attacks, impacts, and mitigation strategies are presented.

The roadmap of this work is as follows. Section II presents the adversary and attack models. Sections III and IV outline the protocol- and device-level vulnerabilities, the corresponding cyberattacks, and potential impacts and mitigations. Section V concludes the paper and provides a brief discussion of DER cybersecurity metrics and future challenges.

II. Threat Modeling

This section identifies high-value targets in DER-integrated systems and attack vectors with their corresponding cyberthreats. Assumptions about adversary capabilities and knowledge, and attack specifics following the threat model methodology are introduced in [35]. According to MITRE's ATT&CK for industrial control systems (ICS) framework the distinction between the *adversary* and *attack* models is crucial. The former allows us to evaluate a threat incident from the *"what could happen"* attacker viewpoint, instead of the *"what did happen"* defender's angle. The attack model, describes the requirements for a vulnerability to become a system threat [36]. We compile the threat vectors and the methodology followed to materialize attacks (Table II), and provide cyberattack definitions which are used in Sections III and IV.

A. Adversary Model

The following discussion delineates the assumptions followed in this study regarding the adversarial system knowledge and capabilities, and how they correlate with attacks targeting DER grid communications and devices. Adversaries could rely on publicly available open-source intelligence information to perform their attacks [37]. Additional knowledge can be acquired after a system asset or device is compromised and/or while a cyberattack is propagated in the system. Knowledge can also be obtained by accessing unsupervised hosts on enterprise networks [34], [38], by gaining unauthorized access to data shared among DER devices. Other methods include eavesdropping, intercepting exchanged data [39], IP identification and port scanning, application-level protocol exploitation [38], [40], ciphertext decryption, or malicious insiders.

Equally important to the attacker knowledge assumptions are the adversarial capabilities (i.e, *"what could happen"*). Adversarial capabilities consider the access to DER assets within a given system. For example, an attacker might be able to connect to remote DER devices through legitimate Bluetooth or speedwire connections (i.e., insider case) [41]. Additionally, attackers could possess or have physical access to EV charging stations or to the local area network (LAN) over which DERs communicate [42]. In the latter case, such access could be achieved if attackers can infiltrate the LAN using proxy attacks on PCs, routers, surveillance systems, etc. [43]. Additionally, other attacks assume that the adversary is capable of compromising peripheral controllers and deploying custom firmware [44], [45] (e.g., change voltage measurement values in human-machine interfaces (HMIs) [40]). As a result, attackers can remotely manipulate and jeopardize various physical assets (e.g., distribution level devices, DERs,

TABLE II: Attack vector description and potential threats for DER assets.

Attack vector	Description	Threat
Lack of interoperability	DER architectural diversity and implementation specifications (e.g., security requirements) can result in inter-system insecure communications.	DER denial of legitimate messages and control commands
Data integrity violations	Stored, transmitted or received data is modified without validation, causing DER malfunction or allowing unauthorized access to control/log information.	Malicious modification of control parameters
Implementation errors	Security flaws within systems and/or communication modules enabling the remote control of DER assets and exfiltration of historical generation data.	Command and control of load/demand-side devices
Supply-chain compromises	Installment of malicious hardware-based eavesdropping programs, worms, oversights during manufacturing of components, devices, or systems.	Sensitive information disclosure
Insecure firmware	Digital signatures of firmware updates are not verified, granting malware (viruses, worms, trojans, etc.) access to otherwise secure systems.	DER systems privilege escalation

substation equipment, etc.) [37]. Attackers are assumed to have sufficient computational resources – especially when supported by criminal organizations or nation-state actors – to crack passwords and decrypt power grid data. For example, it is reported that by brute-forcing PIN codes of wind farm control panels, attackers could send malicious commands to wind turbines impacting grid operation [42].

B. Attack Model

The attack model specifics are essential for the threat model description (e.g., in retrospection of past cyberattack incidents). Although we do not provide one-to-one mappings between attacks (presented in this study) and each corresponding attack model component, their key aspects – influencing impacts and mitigation strategies – are described in Sections III and IV. Attack model information is crucial when establishing the requirements for a vulnerability to develop into a system compromise, its potential impact, and mitigations or other methods to overcome such adversity. Following the attack methodology in [35], the attack model can be considered as being composed of the following six elements, *i)* the attack frequency, *ii)* the attack reproducibility, *iii)* the functional level being attacked in the system, *iv)* the attacked asset, *v)* the techniques being used, and *vi)* the attack premise. For instance, some attacks might have to be performed iteratively and reproduced multiple times to compromise the system behavior. This could be the case with packet replay, DoS, and MitM attacks, where attacks might aim to spoof DER communications or exhaust DER protocols and/or device resources causing intermittent, slow, or loss of communication thereof [46]. The attack functional level and the targeted DER assets notably differ when considering communication protocol and device attacks. Typically, cyberattacks targeting DER devices could be assigned to levels 0 and 1 including process sensors, actuators, and controllers, while attacks on the communication, coordination, and control fabric of DER systems target the higher levels (i.e., 3, 4, and 5) of the Purdue model [47].

Distinctions are also necessary when investigating the attack techniques and the premise of cyberattacks. A detailed presentation of the most common and recent attack techniques used by adversaries can be found in [36]. The attack premise delineates whether the attack is performed in the cyber or physical system domain. For our study, identifying the attack premise is fairly intuitive since DER protocol attacks are limited to the cyber domain, while DER device compromises could span both the cyber and the physical domains. Information on how complex cyberattacks could target the cyber and physical domains while exploiting diverse attack techniques is provided in [35]. Specifically, in the case studies presented in [35], physical devices, e.g., inverter controllers, are compromised by exploiting control logic modification techniques impacting power conversion, power factor, active/reactive injections, etc. Additionally, cyberattacks targeting communications – via time-delay attacks on the cyber domain – and the impact of intercepted, delayed, and/or modified control commands on the simulated power system models are also demonstrated.

C. DER Targets and Cyber-Threats

We refer to mission-critical system assets which can jeopardize grid operation if maliciously compromised by threat actors as *crown jewels* [48]. Crown jewels span the ICT infrastructures, such as the stakeholder-to-DER device communication channels [46], physical-interfaces [43], and the DER devices themselves. Notably, DER devices include PV inverters or smart inverters [40], BESS, EVs, wind turbines [42], demand-side loads [49], and DER controllers. Gaining access to any crown jewel, enables adversaries to manipulate DER power output (e.g., generated, stored, etc.), which can result in possible brownouts, false trips, feeder overloadings, voltage/frequency violations, damaged protection equipment or system instabilities [26].

We distinguish between attacks targeting the DER communication protocols used for the control and coordination of DER assets, and the actual DER embedded devices and their components, i.e., hardware, and software. Although the threat surface for these two categories might share similarities, it also has differences (e.g., attack access, exploitation tactics and techniques, etc.). Along with these differences, the interoperable nature of DER systems mandates comprehensive security mechanisms that treat the DER crown jewels jointly. Table III compiles common cyberattack definitions relevant to DER asset vulnerabilities.

III. DER Protocol Level

The following section elucidates DER protocol-level security oversights and furnishes approaches to mitigate and overcome the impact of intrusions exploiting the communication plane. We systematically examine prominent industrial control protocols and demonstrate the DER cyber kill chain indicating the steps adversaries follow to compromise EPS operations.

A. DER Protocol Level Vulnerabilities

The most commonly used protocols for DER communication include the IEEE 1815-DNP3, Modbus, OpenADR, and IEEE 2030.5 [53]. However, most of these protocols

TABLE III: Definitions of cyberattacks tailored for DER assets.

Attack Type	Definition	Reference
Network Reconnaissance	Adversary performs vulnerability scanning on a network. Information such as IP/MAC addresses of DER devices, open ports, services running, and type/version of the system can be disclosed.	[46]
Eavesdropping	Attacker "listens" to confidential in-transit data potentially stealing sensitive information.	[50], [51]
Man-in-the-Middle (MitM)	Adversary redirects communication through compromised "middle" node (e.g., network switch, gateway, etc.) enabling packet monitoring and modification before they reach their destinations.	[4], [34], [51]
Denial of Service (DoS)	Target resources are overloaded (ports are flooded with traffic), inhibiting its nominal operation. Targeted devices become "laggy", unable to timely issue responses to legitimate device requests.	[46]
Packet Replay	Data transmissions between DER client applications and the DER devices are recorded, modified, and retransmitted by attackers at different time instances.	[46], [52]
Supply-chain	Adversary adds malware during the manufacturing, system integration, shipping, or installation stages. The malware can be weaponized remotely to perform unauthorized/unintended actions.	[34]
Brute forcing and fuzzying	Adversary attempts to guess credentials, encryption keys, etc. or bring the system to an unexpected state. Once successful, he/she could attain unauthorized access to system resources.	[52]

did not originally support any overarching cybersecurity requirements [54]. Specifically, Modbus and DNP3, two widely used serial protocols in process automation systems, have several identified vulnerabilities. For instance, the authors in [30], provide a comprehensive attack taxonomy for DNP3 and discuss 28 different attack types. The presented attacks can be classified into four broad threat categories, including DNP3 data *i)* interruption, *ii)* interception, *iii)* modification, and *iv)* fabrication attacks. Interruption and interception attacks could delay control commands to industrial assets or acquire data in-transit. However, modification and fabrication attacks arise as the most threatening since they can send erroneous data to affect industrial processes, alter device configurations, and spoof master controllers, as shown in Fig. 4. The attack impacts range from the acquisition of network and device configuration data to the corruption of remote devices and acquiring control of DNP3 master units. Similarly, more than 700 vulnerabilities have been identified in the open source CERT Java-based implementation of OpenADR [55]. Some of those vulnerabilities could be remotely exploited, compromising sensitive data such as usernames, system properties, installation directories, etc [56].

To enhance the security of DER communication, IEEE 1547-2020 interconnection and interoperability standard identifies the security requirements to be satisfied by both communicating parties [57]. Although compliance with IEEE 1547 can safeguard the exchanged data and control commands issued between DERs and aggregators, cyberattacks aiming to disrupt grid operations (e.g., DoS) remain. Of the aforementioned DER protocols, only IEEE 2030.5 was developed with stringent cryptography requirements [58]. The latest versions of DNP3 [59], Sunspec Modbus 700 series [60], and OpenADR 2.0 conform with IEEE 1547-2020 and National Institute of Standards and Technology (NIST) requirements. As such, they can be seen as semantically identical from a security standpoint with IEEE 2030.5 [60]. Furthermore, transport layer security (TLS 1.2 or 1.3) is advised for all protocols to enhance wireless communications security between aggregators and DER edge devices [52], [61].

Although there are secure communication protocols, the network communication infrastructure remains a prominent threat vector for adversaries. This can be attributed to the hesitation of industrial facilities to switch to newer and more secure communication protocols considering the potential

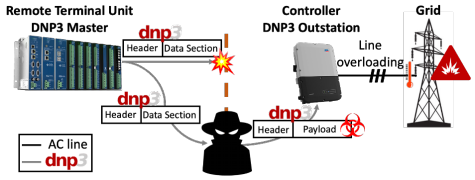

Fig. 4: DNP3 attack on DER controller: attacker intercepts the control command (from master) and issues a maliciously fabricated command to the outstation device.

economic or operational overheads. The plethora of legacy devices is also a limiting factor that restricts the modernization efforts of the communication fabric. The situation is further exacerbated since according to the Electric Power Research Institute (EPRI), more than 75% of North American electric utilities use the DNP3 protocol for industrial control applications and supervisory control and data acquisition (SCADA) systems [62]. For instance, attacks targeting DNP3 communications could either aim to exploit vendor implementations of the protocol, protocol specifications, or vulnerabilities in the supporting communication infrastructure [30]. In addition to DNP3 protocol vulnerabilities, the user datagram protocol (UDP) vulnerabilities arise since, in some systems, portions of DER modification requests are passed in plaintext [26], which presents a critical control vulnerability to the DER system.

Applying the latest protocol versions using TLS and cryptographically secure communication channels can potentially deter adversaries. However, the security of the power grid system is contingent upon each weakest link. Knowing that many already deployed DER devices support insecure and outdated versions of the aforementioned communication protocols, limited computational capabilities prohibiting the implementation of sophisticated encryption algorithms or even updating their firmware (e.g., could be infeasible due to field operational constraints), urges for potent attack detection and mitigation mechanisms. Following, we discuss some of the eminent cyberattacks exploiting the pitfalls of protocol vulnerabilities.

B. DER Protocol Level Attacks

To identify which layer of the protocol stack is targeted by each attack, the Open Systems Interconnection (OSI) basic reference model is used [63]. The OSI model has seven major layers: application, presentation, session, transport, network, data link, and physical layer. In this paper, we focus on the security of commonly used industrial control protocols and

specifically consider the data link, network, and transport layers of the OSI stack. The physical layers as well as the session, presentation, and application layers are not discussed since no security requirements are defined for the physical layer (bit transmission layer), while the aforementioned higher OSI layers can be application-specific or supported by other application protocols (e.g., secure file transfer protocol – FTP/SFTP, simple network management protocol – SNMP, telnet, etc.).

Data link layer uses the Ethernet protocol which is vulnerable to media access control (MAC) spoofing attacks. MAC addresses can be spoofed, allowing Ethernet frames to be forwarded to adversaries [41]. In addition, MAC flooding attacks target the MAC address tables used by switches to store the information of legitimate devices, and the specific ports to which each device is connected [41]. On the network layer, the cybersecurity of DER device communication is specified by IEEE Std. 2030.5, which operates over the UDP and transmission control protocol (TCP) with support for IPv4 and IPv6 protocols [52]. Many owners of DER devices can remotely communicate with their DER devices and receive data such as measurement statistics, network communication analysis, firmware updates, and more.

Especially for Modbus and DNP3, multiple attacks have been reported that compromise the confidentiality, integrity, or availability of in-transit data. In [31] 28 attacks targeting Modbus TCP packets and 20 attacks targeting Modbus serial instances are reported. Threat actors with network access, can intercept, interrupt, modify and fabricate Modbus control packets causing DoS, and/or injecting bad data and malicious commands resulting in loss of situational awareness and asset controllability. Similar attacks on DNP3, i.e., packet interception, fabrication, etc., are reported in [30] focusing mainly on the data link and transport layers, achieving loss of confidentiality, awareness, and control of industrial assets. In [38], the authors demonstrate the feasibility of attacks that corrupting manufacturing message specification (MMS) communications (facilitated by IEC 61850) by reporting false inverter limits curtailing the power generation of DER assets.

Attacks targeting UDP vulnerabilities, during client-to-DER device communications, such as packet replay attacks have also been reported [26]. During a successful packet replay attack, the plaintext requests are captured while being transmitted. The attacker can then send the captured packets and issue malicious commands to the DER, resulting in device malfunctioning. For IPv4/IPv6 protocols, possible attacks include, network reconnaissance, packet replay, MitM, and DoS [46]. Sophisticated MitM attacks on client applications and DER device communications have multiple steps. First, the adversary eavesdrops on the DER-to-client communications and then performs address resolution protocol (ARP) poisoning and port stealing attacks [46]. ARP poisoning forces the MAC address of the adversary to be linked to the IP address of the target. This technique enables the interception of data in transit. Port stealing enables the interception and modification of data by the adversary before it is delivered to the destination.

On the transport layer, the predominant attack is synchronization (SYN) flooding. SYN flooding is a type of DoS attack where the adversary sends continuous SYN requests to multiple ports of the target device using fake IP addresses [41]. The target device sends acknowledgment packets (SYN-ACK) to each fake IP request. Since no consequent actions are performed by the fake IP client, the target device's port remains open until the connection times out.

C. DER Protocol Level Impacts

The MAC spoofing attack on the data link layer aims to give adversaries unauthorized access to the network by maliciously modifying the source IP address [41]. Another attack on this layer, MAC flooding, can target DER devices such as inverters, which can result in memory overuse and potential communication bottlenecks. The adversarial impact could lead to loss of availability in communication with the DER device, including the inability to control DER power management parameters.

MitM and packet replay attacks on the network layer of DER device communication leverage the commands received from client applications using UDP/IP transport protocols. Such interception has been reported in [46], where sensitive information involving DER generation data and control commands were exchanged in plaintext format. Traffic analysis and in-transit packet inspection can be used to exfiltrate setpoint values. The underlying impact of a successful packet replay attack is demonstrated in [3], where the replay attack doubles the magnitude oscillations of the DER's real output power. In microgrids, especially during autonomous operation, such disturbances could result in relay trippings, damaged equipment, and potentially load shedding events [64]–[66].

The impacts of protocol-based DoS attacks, e.g., during SYN flooding, could diminish the availability of DER devices. Reference values for real/reactive power and phase measurements are critical for the operation of inverters. If such information is delayed, real-time reference values cannot be updated, and thus the DER operation is indicated by firmware-defined defaults [3]. Such distortions can result in under- or over-generation, leading to uneconomic operation, and real or reactive power instabilities in the DER connected grid [67].

D. DER Protocol Level Mitigations

Different mitigation strategies for protocol-level attacks have been reported in the literature [41], [68]. To mitigate spoofing attacks on the data link layer, authentication-based access control is necessary. In the presence of authentication-based access control, the communication between the client and the device has to be first authenticated before the client is allowed to connect and exchange data and control commands. An alternative proposed mitigation approach considers the network switch configuration, i.e., white-listing a limited number of trusted MAC addresses, while discarding requests from unknown sources. Network switch best practices suggest the deployment of an authentication, authorization, and accounting server, that manages connections and certifies that the MAC addresses are added to the table only after being authenticated.

On the network layer, the use of firewalls, one-way communication diodes, packet filters, circuit-level gateways, proxy servers, and two-way authentication can be utilized to prevent network reconnaissance, packet replay, MitM, and DoS attacks. The use of physical and logical network segmentation

and perimeter security defenses can be used to prohibit access to critical parts of the system and prevent the lateral movement of threat actors between IT and ICS networks (if the prior is compromised) [69]. Demilitarization zones should also be enforced to aid network segregation and serve as proxies, avoiding the security hazards that network-connected devices could port to DER control functionalities. DER applications using TCP/IP are more resistant to packet replay attacks since unique session IDs are generated during the initial three-way TCP handshake (communication initialization) [46]. TCP/IP transport includes additional IP header information that DER applications can use to prevent packet replay attacks. Leveraging the unique IP headers, the server is able to detect and drop duplicate packets, hence preventing packet replay attacks.

Furthermore, the implementation of cryptographic techniques, secure key distribution, and exchange schemes can help prevent MitM and replay attacks [70]. Currently used cryptographic mechanisms might no longer be secure once quantum computers become widely available, and EPS stakeholders will have limited time to adapt their systems [71]. To address this issue, quantum key distribution (QKD) schemes have recently been proposed to improve the security of cryptographic keys [72], [73]. Contrary to other application fields, e.g., computer networks, online banking, etc., the power systems community has only recently started considering such approaches, and this can be mainly attributed to the fact that QKD schemes cannot be directly applied to deployed and legacy systems. In addition, testbeds to evaluate the real-time performance of such quantum schemes do not exist. However, in the future, it is evident that quantum-secure encryption algorithms, QKD schemes, and the essential infrastructure to test them would be part of EPS cybersecurity research [74].

On the transport layer, mitigation of SYN flooding attacks is achieved by cryptographic hashing and stack tweaking, which reduce the connection request timeout period dropping incomplete sessions. Cryptographic hashing will determine the legitimacy of the connection by sending the SYN-ACK packet with a code derived from the client's IP address, port number, and unique ID number. Dropping incomplete connections in stack tweaking frees up ports for legitimate connections. Firewalls, intrusion detection and protection systems (IDS/IPS), and traceback and push-back services can limit excessive traffic, therefore countering DoS attackers. Fig. 5 presents the DER cyber kill chain, where we recapitulate protocol vulnerabilities and attack entry points, enumerate potential attack impacts, and mitigations to overcome adversities.

IV. DER Device Level

Different DER categories can be identified based on their operation principles, thus, DER device compromises can impact grid operations to varying degrees based on their category and system utilization. This section focuses on vulnerabilities, attacks, impacts, and mitigations on the DER device-level.

A. DER Device Level Vulnerabilities

Inverter-based resources are rapidly deployed in EPS on a commercial and residential scale. However, they remain vulnerable to cyberattacks that can modify or erase their default DER settings [49]. Rooftop PV inverter control, for instance, is regulated both on the local level (primary) as well as at a higher level, i.e., secondary control. The primary control system is responsible for matching the inverter-generated energy to the consumer power demand. Contrary to the local control system which operates on the consumer side, centralized secondary control resides on the concentrator/aggregator and utility sides. The secondary control system orchestrates inverter operation on a larger scale, by managing ancillary services and providing setpoint updates to local control systems regulating frequency and voltage deviations after a perturbation, e.g., load change, fault, etc., has occurred. Typically, these control systems are operated remotely, using Internet-of-Things (IoT)-based and third-party applications, which could expose such DER devices to cyberattacks. For example, in [46], the authors demonstrate that by eavesdropping DER communications (performed over the Internet), passwords, user data, serial IDs and device names can be extracted using network traffic analysis software (e.g., Wireshark). Furtheremore, in some cases, sensitive information is exchanged in plaintext format, highlighting the importance of end-to-end data encryption and endpoint security hardening on the physical device itself.

Similar security concerns exist for wind turbines which represent another significant DER type. Wind turbine control panels (WTCP) are used to control turbines and monitor their real-time operating conditions, e.g., their generation setpoints are dynamically controlled to meet the electricity demand. According to [42], in some deployments, the only security practices employed against adversaries attempting to access the WTCPs are software-based credential authentication (e.g., passwords, identification number, PINs, etc.). Standalone credential authentication is not considered secure, granted that it can be bypassed using brute forcing and fuzzing techniques. Additionally, phishing, spear-phishing, vishing, etc., and other social engineering campaigns have also managed to exfiltrate sensitive authentication data from operators potentially jeopardizing the secure operation of wind-based DERs.

The electrification of the transportation sector is a major thrust towards grid decarbonization. As a result, a precipitous growth has been observed in the number of EVs across the world. EV batteries can be used as backup power supplies during unexpected and instant power demand. To support such ancillary backup services, as well as to charge their battery resources, EVs connect to the electric grid via charging stations. According to [75], EV charging stations (EVCS) first, authenticate the EVs, and then they either charge them or connect them to the main grid to be used as ad-hoc energy storage. Authorization can be done through radio frequency identification (RFID), Bluetooth, or Wi-Fi technologies. However, RFID systems have been proven to be insecure and are vulnerable to malicious attacks such as eavesdropping and active interference [76]. RFID readers and tags operate in noisy environments, which decreases security and can consequently compromise the EVCS. Furthermore, authorization done using wireless networks (Wi-Fi or Bluetooth) can be exploited by adversaries as well. Multiple design flaws, security weaknesses, and practical attack scenarios have been reported regarding Bluetooth technologies, enabling adversaries to pair

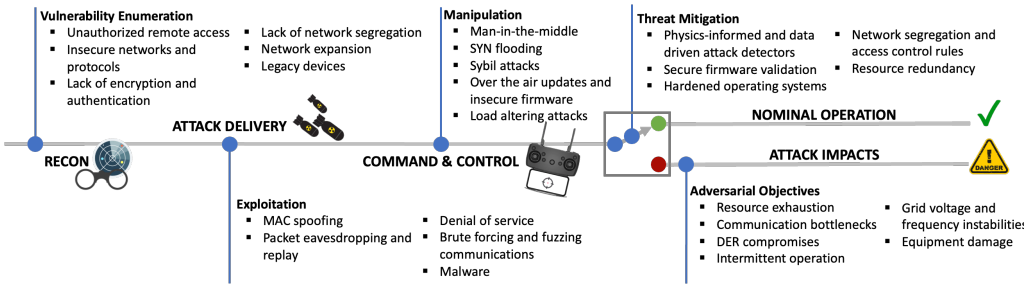

Fig. 5: DER cyber kill chain including communication layer vulnerabilities, attacks, impacts, and mitigations.

to devices and impersonate legitimate users [77]. Apart from the authorization and wireless network configuration security oversights, in [78] the authors present the vulnerable components of EVs that could be exploited by adversaries (e.g., remote attacks) compromising grid operation.

Apart from the discussed vulnerabilities concerning generation-type DERs, critical vulnerabilities in DER controllable loads also exist. The IoT is a network of connected devices including smart appliances (e.g., smart thermostats, air-conditioning, heat pumps, EVCS points, etc.), enabling the exchange of information between devices and users leveraging wired and wireless connections [79], [80]. These IoT-enabled devices are connected to the load-end of DERs and their operation is typically orchestrated remotely by their end users. According to [79], [81], a large number of IoT devices (using remote internet access mechanisms) still lack concrete security mechanisms and, as a result, can be vulnerable to cyberattacks. Researchers have demonstrated that attackers can manipulate IoT-connected devices in low-inertia EPS (e.g., relying on renewable generation) and other exogenous conditions to cause unsafe grid operation. That is, in [80], [82], the authors investigate the impact on grid stability of load altering attacks – if multiple IoT-connected high-wattage devices are compromised simultaneously – during the COVID-19 lockdown period. This adversarial behavior is enabled by the absence of overarching defense mechanisms, such as anti-viruses, and the sporadic provision of software/firmware updates and security patches which further weaken the device security posture. As a result, the vulnerabilities of such IoT-connected devices can be ported to the utility grid, given their interconnection to DERs.

The authors in [83] report that another compelling reason undermining IoT – and DER-controllable load – security is that during the design cycles, function and lowering manufacturing costs were prioritized above firmware security. As a result, end-users are presented with feature-full devices with multiple backdoors that adversaries can exploit; paving the way for malware developers [83]. Smart thermostats, for example, represent a prime example of how the consequences of a compromised IoT device could propagate, posing threats to the power grid. Smart thermostats regulate the temperature of residential or commercial facilities by "cleverly" managing heat sources and air conditioners. Thermostats can learn their users' patterns and adapt their operation accordingly. The cybersecurity of such devices has been shown to be lacking since many are shipped from manufacturers using default configurations and predefined credentials [79]. Furthermore, the end-users of such devices might be unaware of the essential steps secure their devices against cyberattacks. Consequently, such devices are left vulnerable to attacks that could simultaneously trigger on/off particular loads (e.g., heaters) deliberately affecting the instantaneous power demand of power grids, leading to blackouts or brownouts [4].

Similarly to IoT-based systems which leverage ICTs to exchange information, recently the design of solar farms has also incorporated "smart" features. In large solar deployments, ICTs are used for the remote and real-time management of the generated power used for economic dispatch and demand-response schemes. Centralized storage solutions are also used for the aggregation of historical and generation data, exposing solar farms to threats (e.g., single-point-of-failure paragon). The remote control, communication, and data aggregation features of grid resources can be exploited as attack entry points. This was the case with the cyberattack targeting VESTAS offshore wind turbine manufacturer, which led to the ex-filtration of sensitive data and "*forced VESTAS to shut down IT systems across multiple business units and locations to contain the issue*" [84]. Although, according to the Danish wind manufacturer, customers were not affected, the socio-economic and reputation blow to the company was acute.

In residential solar deployments, communication technologies such as Bluetooth are used regardless of the limited cybersecurity mechanisms, which can result in security breaches compromising user privacy [49]. Aside from the attacks on IoT controllable loads and generation assets that stem from inherent implementation or architectural vulnerabilities, the possibility of supply-chain-based attacks should also be considered. Security oversight in manufacturing facilities can be exploited to develop supply-chain attacks, in which adversaries are granted apriori control over thousands of DER-connected assets [85]. The possibility of supply-chain compromises along with the catastrophic consequences of such events was demonstrated during the colonial pipeline incident in 2021 [21].

B. DER Device Level Attacks

Attacks targeting the DER device level exploit implementation, architectural, and other security design oversights (e.g., communication, internal storage, remote update or control functionality, etc.) to maximize their impact and compromise EPS operations. In the case of inverters, for example, after successfully gaining access to the DER assets, adversaries can launch cyberattacks including, *i)* DoS attacks compromising the inverter's availability, *ii)* data alteration attacks where the exchanged data between DERs and utilities are maliciously modified, and *iii)* command injection attacks where termination commands or malicious controls are forwarded to the

inverters [38], [86]. During DoS attacks, the communication bandwidth of the inverter can be flooded leading to disruptions, i.e., the process control flow of the device is suspended [46]. Inverter operation is dynamically regulated to enhance power generation efficiency and support ancillary services when requested by grid operators. However, adversaries could delay or prevent the transmission of critical data (e.g., sensor measurements, control commands, etc.) to certain DERs inhibiting their operation [46].

MitM attacks can also be leveraged to compromise grid inverters. In such scenarios, attackers can gain device-level information by eavesdropping on data traffic between inverters and the utility grid. Attackers can access system information by decoding MMS real-time data packets [40]. Given that most inverter models use MMS to send and receive data, such attacks could have a considerable impact on grid stability. Attackers could compromise the DER operation by modifying the inverter configuration using undesirable parameters, e.g., tampering with the reactive power references [87]. Brute force attacks can also be leveraged to compromise DER assets. In [42], researchers demonstrate that adversaries can brute force weak PIN sequences and get access to WTCPs. Similarly to the inverter command injection attack, adversaries can send malicious commands to wind turbines, modifying setpoints or control objectives, causing unexpected operations [88].

In many cases, DER assets are owned by end-users, interfaced to user networks, and exhibiting similar operation to common IoT devices. As such, DERs could be remotely operated and controlled by consumers or other third-party applications. IoT devices have been exploited on a massive scale in the past, as was the case with the Mirai botnet attack [79]. The Mirai malware, after its propagation to multiple vulnerable IoT devices, grants adversaries full control over the compromised devices. Groups of compromised devices, i.e., botnets, can then be collectively exploited to cause distributed DoS (DDoS) attacks [89]. However, in the case of DERs, such attacks could severely affect grid stability. Apart from botnet attacks, other IoT-sourced vulnerabilities could be also abused.Threat actors can perform replay attacks by replicating legitimate commands transmitted from DER asset owners. RFID authentication and Bluetooth or Zigbee communication packets can be eavesdropped and replayed, enabling unauthorized access to DER devices [90]. The security of these IoT-connected DER devices is relied upon the user competence in safeguarding their assets. If IoT network security is overlooked, adversaries could capture exchanged data, obtain session or encryption keys, access the devices, and issue commands to render DERs unreachable (DoS) or instruct anomalous operations [90].

C. DER Device Level Impacts

Adversaries, after gaining initial access to DER devices, can follow different approaches to deploy their attacks [36]. If maximizing the *immediate* system-wide impact is the objective, overvoltage or undervoltage conditions, frequency fluctuations, false trippings, and disconnection mechanisms could be targeted. Power systems have built-in mechanisms to automatically detect and isolate such high-impact events to limit their consequences. Different detection approaches (e.g., physics-based, data-driven, or a combination of the two) could be used to overcome such conditions [40], [91], [92].

On the other hand, in the advanced persistence threat (APT) case, threat actors might prioritize system persistence, breach of privacy, and long-term system degradation instead of immediate impact, and opt for more sophisticated and stealthy attacks [93]. For instance, attackers could exploit firmware vulnerabilities and achieve remote access on DERs through public-facing applications or the supported remote services [36]. While in control of the DER device, attackers can stealthily perform minute modifications to system parameters or coordinate attacks in ways that will not affect the net system behavior deceiving detection mechanisms [94], [95]. Such stealthy attacks might cause unsafe, unstable, or uneconomic operation of IBRs. Adversaries could also exfiltrate sensitive user information (e.g., credentials, passwords, etc.), since DER devices might be connected in user-owned home networks. Attackers may also be learning the operational patterns of DERs, that is, aggregating enough system information to identify the temporal and spatial conditions which, if satisfied, can maximize the impact of attacks on the grid [94], [96].

The rapid adoption of EVs (from 3 million in 2017 to 125 million by 2030 [97]) makes them prominent targets for attackers aiming to gain access to EVs or EVCS. Malware can be deployed and propagated throughout the whole EV infrastructure, compromising the charge controllers, demand-response schemes, charging limits, grid power quality, and crippling the power and transportation sectors. According to [37], compromised EV supply equipment (EVSE) servers can prevent EVCS sessions by denying authentication, or reproducing incorrect information about charging station data (e.g., price, online station status, etc.). Furthermore, EVCS being high-wattage assets, if maliciously manipulated in addition to power-related consequences (e.g. increased load demand, power quality issues, etc.), can also inflict considerable financial losses on electric power utilities [98]. Similarly, sensitive user information (e.g., identity, location, payment information, etc.) could be leaked during potential attacks on the EV and charging infrastructures [99]. The absence of attack impact assessment methodologies for EV networks is highlighted by the authors in [100]. Their work attempts to identify potential attack and failure scenarios while demonstrating the consequences of such events on the corresponding EV system security.

Researchers have demonstrated that there are multiple paths to compromise the security of wind-integrated DER assets. In [42], access to WTCP is granted by launching a brute force dictionary attack on the WTCP device. Similarly, in [88], by compromising network devices and wind process automation controllers, malicious requests can be sent to turbines, preventing nominal operation and potentially causing damage to critical electrical and mechanical components. The impacts of such attacks can lead to fires, explosions, jeopardize personnel assigned to resolve such issues, and the safety of surrounding communities [101], [102]. The aforementioned high-profile wind incidents might have not been caused by cyberattacks, but the probability of exploiting

wind turbine vulnerabilities remotely exists. Furthermore, the impact that attacks on wind turbines could have on grid reliability has been investigated in the literature [103], [104].

Malware, such as the Mirai and its derivatives, or other supply-chain exploits (e.g., hardware trojans, vulnerabilities in commercial and open source software) could be leveraged to control the operation of IoT-connected DERs leading to intermittent operation and DDoS attacks [105]. As a result, the botnet of the compromised DER devices can be maliciously operated as a distributed load or generation. Grid instability can thus occur when DERs and other remotely controlled high-wattage devices (i.e., smart thermostats, EVs, EVSE, Heating, Ventilation, and Air Conditioning – HVACs, etc.) are simultaneously switched on or off, severely affecting the electricity power demand [106]. In large-scale demand-side attack scenarios, grid operators will be forced to perform load shedding to sustain critical loads [82]. Consumers might experience brownouts and service interruptions, while the impacts of load-altering attacks on the local power supply will also affect demand-response schemes [107]. In addition to grid impacts, infected devices could also propagate malware (in a worm-like fashion) to the rest of the devices residing within the same network (e.g., switches, personal computers, mobile phones), thus, jeopardizing sensitive user information [108].

D. DER Device Level Mitigations

To combat threats targeting DER devices, a multitude of mitigation strategies have been proposed. With respect to inverters, the authors in [26] suggest that an additional power electronic interface (energy buffer) should be developed and placed at different locations within the distribution grid (mainly at points where the device is connected to the grid). This energy buffer interface can help avoid unintentional islandings, which could be triggered due to the conflicting anti-islanding detection and low/high voltage ride-through functions that inverters support. The micro-architectural hardware components of inverter controllers have also been utilized for the detection of malicious events within the DER asset's process control loop [44]. In [109], the inherent physical properties of DER-integrated grid systems are used to identify potential actuator or sensor modifications which could lead to abnormal system operation. Furthermore, a multitude of model- and data-driven anomaly detection methods have also been proposed to identify compromised DER assets [110]. Once intrusions have been efficiently detected, the compromised assets are isolated and the available grid resources are utilized to achieve resilience and maintain the power supply-demand balance equilibrium [111], [112].

The prevention of adversaries from launching DoS attacks on EVSE can be achieved via the use of hardened operating systems [113]. Such systems can be leveraged to deploy and keep the EVSE with up-to-date firmware. Furthermore, roll-back firmware update functionality is essential, enabling the use of previously working firmware, in cases where the updated firmware versions are proven unreliable or have been maliciously modified. Different methodologies have also been proposed for the mitigation of the harmonic interference of EV-related cyberattacks. For instance, the authors in [114] and [115], propose pulse-width-modulation and a high-frequency resonance scheme, respectively, that can mitigate the power quality degradation introduced by EVs and bidirectional grid-tied converters (e.g., battery storage). On the other hand, a power management framework leveraging renewable resources and the EV infrastructure itself is used in [116], in order to alleviate power quality challenges encountered in unbalanced distribution networks. The importance of cyber insurance against cyberattacks on EVCS has also been highlighted by researchers. In [98], the authors demonstrate that defense mechanisms and cyber insurance policies can effectively reduce the financial impacts of cyberattacks and curtail insurance premiums for the entities that manage EVCS.

Towards mitigating brute force attacks targeting weak credentials used by WTCP, [113] recommends the usage of password management systems. Furthermore, monitoring user behavior (e.g., failed login attempts), network segregation, and role-based access control rules are encouraged. To mitigate stealthy attackers who aim to gain access to wind turbine controllers exploiting their remote firmware update capabilities (e.g., over-the-air updates), in [117] and [118] different methodologies are proposed to verify firmware trustworthiness. In [117], a secure firmware update scheme is introduced, where devices leverage the blockchain to check for new firmware versions and validate their integrity before downloading and installing the firmware images. On the other hand, in [118], the authors leverage a hardware architecture to validate firmware authenticity. Cryptographic modules are utilized to guarantee the integrity and authenticity of firmware packages.

When viewing DERs from the IoT perspective, most of the security implications and attack mitigation strategies applicable for IoT end-devices could be exercised. In [119], the authors suggest the use of a personal security application (PSA) as a countermeasure. PSA resembles a combination of security features, such as access control mechanisms, malware detection, network traffic, and resource utilization monitoring, etc., to strengthen the security posture of IoT devices and networks. Blockchain technology has also been mobilized to safeguard the security of IoT networks, singling out malicious nodes from benign ones [120]. For example, a blockchain detection methodology is presented in [105] to protect IoT nodes from the Mirai botnet.

On the other hand mitigating supply-chain compromises, hardware- or software-based can be challenging. State-funded initiatives, such as the CHIPS program in the USA are essential to establish "a secure and resilient semiconductor supply-chain that adheres to standards and guidelines on information security, data tracking, verification, and promotes the further development and adoption of such standards" [121]. Furthermore, adhering to recommendations and practices issued by cybersecurity organizations, such as the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), etc. is crucial to mitigate software supply-chain liabilities [13]. In [79], best practices, mitigation techniques, and security policies are enumerated, viewed from the IoT device, infrastructure, communications, and services standpoints which closely match the obstacles that DER infrastructure will have to overcome.

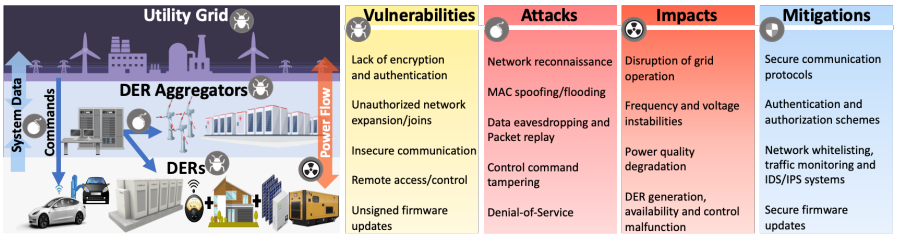

Fig. 6: Overview of DER-integrated electric grid that illustrates how the layered architecture expands the threat surface.

V. DER Cybersecurity Concluding Remarks

Improving EPS cybersecurity and resilience is of critical importance and DERs are expected to contribute toward this effort. However, the sophistication of cyberattacks targeting EPS indicates that multifaceted security approaches should be considered. In Fig. 6 we present potential vulnerabilities at the different levels of the grid architecture, and the impacts of attacks targeting DER devices, aggregators, and utilities. Detection, protection, and mitigation schemes should factor in the inherent vulnerabilities in both DER stacks (cyber and physical) and on every level, from DER assets to system operators. Therefore, security evaluation metrics, which consider how DERs contribute to EPS, are crucial, given the potential risks and system-wide impacts of cyberattacks.

A. Cybersecurity Metrics for DER-integrated Systems

The risks associated with compromises involving DER assets require substantial cybersecurity investments from utilities and aggregators. To justify such investments, metrics are essential for assessing the cybersecurity posture of the involved stakeholders, and the efficiency of the implemented cybersecurity methodologies in curtailing potential risk. In [122], diverse analytical metrics are discussed to assess the resilience of CPS. Similarly, in [123] and [124] cybersecurity and resilience metrics are developed to analyze industrial control systems. Different approaches have been followed to provide qualitative and quantitative metrics to measure the cybersecurity and resilience of power systems [33], [125], [126]. For instance, NIST has proposed a framework that consists of five essential functions to overcome adverse events, namely identify, protect, detect, respond, and recover [127]. For each of these five functions, performance metrics are then employed to assess the ICS security posture using insights from real-world incidents. However, such frameworks fail to measure security holistically since only specific system sections are investigated.

To address this issue, in [128], the authors extend the *R4* resilience framework [129] by introducing a quantitative metrics hierarchy under four main domains, i.e., system robustness, redundancy, resourcefulness, and rapidity. CPS cybersecurity is then evaluated by decomposing each of the four aforementioned domains into subcategories and deriving scores based on asset criticality, interconnectivity, system network topology, and underlying physical processes. A similar path is followed in [130] where a quantitative security metric is proposed that factors the interaction between cyber and physical layers. Then, optimal decisions are made by integrating this security metric in cyber-constrained AC power flow studies.

EPRI highlighting the challenging task of quantifying security in diverse DER architectures has presented a data-driven cybersecurity metric methodology [131]. The proposed metrics framework combines real-world IT and OT data aggregated from the system-under-test. Sixty security metrics, including mean time to discovery, mean time to recovery, threat awareness, endpoint protection scores, etc., are then combined to assess and quantify the cybersecurity status of the system. The sixty metrics are categorized under three core categories (i.e., operational, tactical, and strategic) depending on the operational constraints and security requirements as identified by each stakeholder (e.g., utility, aggregators, etc). EPRI has open-sourced its cybersecurity metrics calculation software, *OpenMetCalc*, which allows users to load their system-specific data and compute their system's performance with respect to these sixty metrics [132]. Based on these scores, executive decisions can be made, and resources can be prioritized to reduce and/or mitigate potential risks. Although this cybersecurity metric endeavor led by EPRI is a step in the right direction, it is still an ongoing research topic that requires active participation from the energy sector.

B. Future Challenges

This work explores the cybersecurity posture of DERs as an essential building block for future resilient EPS. We investigate threats and present an overview of attacks without focusing on specific DER types, e.g., rooftop solar, BESS, or wind turbines. DER vulnerabilities are examined from the protocol and device levels, which are pertinent regardless of the DER type. We furnish a consolidated review of attacks and their potential impacts. Mitigation methodologies and design best practices are also discussed, and in Table IV, we compile a summary of mitigation schemes against different attack types.

Even though the proposed strategies could reduce the DER threat surface, they cannot be considered as "silver bullet solutions". This fact is partly attributed to the DERs' distributed mode of operation, which can be utility-, aggregator-, or prosumer- owned. Especially for the latter case, user negligence in the security configuration of their DER assets, could give rise to compromises. However, the risk and magnitude of such disturbances depend on how many DERs could be attacked simultaneously. Security standards and policies – such as IEEE 1547-2020 [57], NISTIR 7628 [133], NIST SP800-82 [69], CA Rule 21, Hawaii Rule 14 [134], and IEEE 1815.1 [59] – should be enforced ensuring the innocuous DER operation.

The strong coupling between electricity markets, demand response schemes, and DERs can also incentivize the exploitation of DERs for financial benefits. False data injection attacks manipulating measurement points at the distribution level have been demonstrated to be capable of deceiving state estimators and influencing economic dispatch mechanisms [135]. Load

TABLE IV: Cyberattack mitigations and design best practices.

Mitigations	Attacks	Reference
Connection auditing using authentication, authorization, and accounting servers, role-based access control, MAC address white-listing, unused port hardening	MAC spoofing/flooding, DoS, MitM, SYN flooding	[41], [46]
IP header (Sequence number) inclusion in TCP, cryptographically enhanced address resolution protocols (ARP), secure key distribution schemes	Packet replay, DoS, MitM, SYN flooding	[26], [46]
Firewalls, intrusion detection/prevention systems (ID/IPS), traceback and push-back services, cryptographic hashing and stack tweaking	MAC flooding, DoS, MitM, SYN flooding	[26], [52], [41]
Password management systems, access restriction after multiple failed log-in attempts, hardened operating system kernels, roll-back firmware updates	Brute force attacks, DoS, Packet replay, Eavesdropping	[113]
Personal security and privacy practices (e.g., security updates, password managers, encryption, ephemeral keys, etc.)	Packet replay, Eavesdropping	[119]

forecasts can thus be biased, affecting the marginal prices in electricity markets, to benefit corrupt distribution utility operators and DER aggregators. To thwart such attacks, resilient state estimation algorithms [92], and incentive reduction policies should be implemented [135].

Security challenges will still exist, regardless of the preventive and preemptive methodologies that we propose. Developing universal risk management schemes can be a perplexing or infeasible task due to the distributed, ad-hoc (e.g., EVs, battery storage) and stochastic (e.g., solar inverters) nature of DERs. However, comprehensive system modeling using digital twin systems and data-driven approaches can be leveraged to forecast grid behavior and predict cyberattack impacts. Additionally, risk assessment and cyber-physical risk metrics can be used to evaluate and prioritize mitigation decisions. High-fidelity information, derived from system models, can assist risk metric estimations, which can prove useful when designing response strategies and self-healing schemes [136].

The influx of DER devices and their projected numbers underscore the need for comprehensive security practices. To harness DER advantages and withstand their underlying security impediments, the combined knowledge of security engineers, the industry, and academia is essential. User vigilance is also crucial to impede malicious behavior attempting to achieve foothold on user-owned DERs. Security standardization and policy-making procedures can strengthen the cybersecurity posture of DERs and prevent vulnerabilities from materializing into threats. However, if the discussed practices fail to prevent or detect attacks, risk metrics, detailed system modeling, and mitigation plans can orchestrate resources to inhibit or overcome undesirable grid conditions and enhance EPS resilience.

REFERENCES

[1] National Renewable Energy Laboratory (NREL), "Grid Modernization," [Online]: https://www.nrel.gov/grid/, 2021.

[2] North American Electric Reliability Corporation, "Distributed energy resources: Connection modeling and reliability considerations," 2017.

[3] S. Gholami, S. Saha, and M. Aldeen, "A cyber attack resilient control for distributed energy resources," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2017, pp. 1–6.

[4] S. Soltan, P. Mittal, and H. V. Poor, "Blackiot: Iot botnet of high wattage devices can disrupt the power grid," in *27th USENIX Security Symposium (USENIX) Security 18)*, 2018, pp. 15–32.

[5] G. Insights, "Global Capacity of Distributed Energy Resources Is Expected to Reach Nearly 530 GW in 2026," 2017.

[6] H. K. Trabish, "2021 Outlook: The DER boom continues, driving a 'reimagining' of the distribution system," [Online]: https://tinyurl.com/2p96cz4b, 2021.

[7] E. Ghiani *et al.*, "Impact on electricity consumption and market pricing of energy and ancillary services during pandemic of covid-19 in italy," *Energies*, vol. 13, no. 13, p. 3357, 2020.

[8] A. D. Syrmakesis, C. Alcaraz, and N. D. Hatziargyriou, "Classifying resilience approaches for protecting smart grids against cyber threats," *International Journal of Information Security*, pp. 1–22, 2022.

[9] The University of Texas at Austin, "The Timeline and Events of the February 2021 Texas Electric Grid Blackouts," https://energy.utexas.edu/ercot-blackout-2021, 2021, accessed: 2021-9-07.

[10] NIST - National Vulnerability Database, "CVE-2018-0296 Detail," https://nvd.nist.gov/vuln/detail/CVE-2018-0296, 2018.

[11] North American Electric Reliability Corporation (NERC), "Lesson Learned - Risks Posed by Firewall Firmware Vulnerabilities," 2019.

[12] M. Areno, "Supply Chain Threats against Integrated Circuits," https://tinyurl.com/445vx9x6, 2020.

[13] Cybersecurity and Infrastructure Security Agency (CISA), "Securing the Software Supply Chain," [Online]. Available: https://tinyurl.com/2p8c38ev, 2022.

[14] J. Williams, "What You Need to Know About the SolarWinds Supply-Chain Attack," https://tinyurl.com/ys84v9e5, 2020.

[15] NIST, "SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains," https://tinyurl.com/57w3xe5x, 2021.

[16] IEEE, "IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," *IEEE Std 1547-2018 (Rev. of IEEE Std 1547-2003)*, 2018.

[17] Sunspec, "SUNSPEC MODBUS FOR IEEE 1547 ," [Online]. Available: https://sunspec.org/sunspec-specifications-for-ieee-1547/, 2021.

[18] J. Gamblin, "IEC 62746-10-1:2018 Systems interface between customer energy management system and the power management system - Part 10-1: Open automated demand response," [Online]. Available: https://webstore.iec.ch/publication/26267, 2018.

[19] IEEE, "IEEE standard for smart energy profile application protocol," *IEEE Std 2030.5-2018*, pp. 1–361, Dec 2018.

[20] R. J. Concepcion *et al.*, "Effects of communication latency and availability on synthetic inertia," in *2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2017.

[21] N. P. Michael D. Shear and C. Krauss, "Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers," https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html, 2021.

[22] L. Mathews, "Florida Water Plant Hackers Exploited Old Software And Poor Password Habits," https://tinyurl.com/yxakfed4, 2021.

[23] L. Muthuppalaniappan, Menaka and K. Stevenson, "Healthcare cyberattacks and the COVID-19 pandemic: an urgent threat to global health," *International Journal for Quality in Health Care*, vol. 33, no. 1, 09 2020. [Online]. Available: https://doi.org/10.1093/intqhc/mzaa117

[24] NREL, "Distributed Energy Resource Cybersecurity Framework (DERCF)," [Online]: https://dercf.nrel.gov/, 2021.

[25] Sandia National Laboratories, "Renewable Energy & Distributed Systems Integration (RDSI)," [Online]: https://energy.sandia.gov/programs/electric-grid/renewable-energy-integratio/, 2021.

[26] J. Qi *et al.*, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Physical Systems: Theory & Applications*, 2016.

[27] Y. Li and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Transactions on Power Electronics*, 2022.

[28] N. D. Tuyen *et al.*, "A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy," *IEEE Access*, 2022.

[29] J. Ye *et al.*, "A review of cyber–physical security for photovoltaic systems," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 4, pp. 4879–4901, 2021.

[30] S. East *et al.*, "A taxonomy of attacks on the dnp3 protocol," in *Critical Infrastructure Protection III*, C. Palmer and S. Shenoi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 67–81.

[31] P. Huitsing *et al.*, "Attack taxonomies for the modbus protocols," *Int. J. Crit. Infrastructure Prot.*, vol. 1, pp. 37–44, 2008.

[32] M. K. Hasan *et al.*, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *Journal of Network and Computer Applications*, 2023.

[33] J. Johnson *et al.*, "Assessing DER network cybersecurity defences in a power-communication co-simulation environment," *IET Cyber-Physical Systems: Theory & Applications*, vol. 5, no. 3, 2020.

[34] R. Siqueira de Carvalho and D. Saleem, "Recommended functionalities for improving cybersecurity of distributed energy resources," 2020.

[35] I. Zografopoulos *et al.*, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29 775–29 818, 2021.

[36] MITRE, "ATT&CK for Industrial Control Systems Techniques," [Online]: https://collaborate.mitre.org/attackics/index.php/All_Techniques.

[37] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles+ grid data: Is a new cyberattack vector viable?" *IEEE Transactions on Smart Grid*, 2020.

[38] B. Kang *et al.*, "Investigating cyber-physical attacks against iec 61850 photovoltaic inverter installations," in *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*. IEEE, 2015.

[39] Z. Zhou *et al.*, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 43–57, 2019.

[40] A. Teymouri, A. Mehrizi-Sani, and C.-C. Liu, "Cyber security risk assessment of solar pv units with reactive power capability," in *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2018, pp. 2872–2877.

[41] A. Sundararajan *et al.*, "A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security," *Energies*, vol. 11, no. 9, p. 2360, 2018.

[42] A. Zabetian-Hosseini, A. Mehrizi-Sani, and C. Liu, "Cyberattack to cyber-physical model of wind farm scada," in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, 2018.

[43] D. J. Sebastian and A. Hahn, "Exploring emerging cybersecurity risks from network-connected der devices," in *2017 North American Power Symposium (NAPS)*. IEEE, 2017, pp. 1–6.

[44] A. P. Kuruvila *et al.*, "Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids," *International Journal of Electrical Power & Energy Systems*, vol. 132, p. 107150, 2021.

[45] I. Zografopoulos *et al.*, "Time series-based detection and impact analysis of firmware attacks in microgrids," *Energy Reports*, vol. 8, pp. 11 221–11 234, 2022.

[46] C. Carter *et al.*, "Cyber security assessment of distributed energy resources," in *2017 IEEE 44th Photovoltaic Specialist Conference (PVSC)*. IEEE, 2017, pp. 2135–2140.

[47] P. Ackerman, *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*. Packt Publishing Ltd, 2017.

[48] MITRE, "Crown Jewels Analysis," [Online]: https://tinyurl.com/zcuvvdun, 2019.

[49] D. J. S. Cardenas, A. Hahn, and C.-C. Liu, "Assessing cyber-physical risks of iot-based energy devices in grid operations," *IEEE Access*, vol. 8, pp. 61 161–61 173, 2020.

[50] J. Henry *et al.*, "Cyber security requirements and recommendations for CSI RD&D solicitation for distributed energy resource communications," 2015.

[51] I. Onunkwo *et al.*, "Cybersecurity assessments on emulated der communication networks," Sandia Technical Report, Tech. Rep., 2018.

[52] C. Lai, *et al.*, "Cyber security primer for der vendors, aggregators, and grid operators," *Tech. Rep.*, 2017.

[53] J. T. Johnson, "Roadmap for photovoltaic cyber security." [Online]. Available: https://www.osti.gov/biblio/1782667

[54] J. Obert *et al.*, "Recommendations for Trust and Encryption in DER Interoperability Standards," Sandia National Lab, Tech. Rep., 2019.

[55] M. Park, M. Kang, and J.-Y. Choi, "The research on vulnerability analysis in openadr for smart grid," in *International Workshop on Data Analytics for Renewable Energy Integration*. Springer, 2014.

[56] MITRE, "CVE-2010-3860," [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3860, 2021.

[57] IEEE 1547, "IEEE 1547a-2020 - 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," https://standards.ieee.org/standard/1547a-2020.html, 2020.

[58] "Ieee approved draft standard for smart energy profile application protocol," *IEEE P2030.5/D2, March 2018*, pp. 1–358, 2018.

[59] 1815.1-2015, "IEEE Standard for Exchanging Information Between Networks Implementing IEC 61850 and IEEE Std 1815(TM) [Distributed Network Protocol (DNP3)]," https://standards.ieee.org/standard/1815_1-2015.html, 2020, accessed: 2022-05-27.

[60] "SunSpec Modbus Protocol," [Online]. Available: https://sunspec.org/sunspec-modbus-home/, 2020.

[61] "DNP3 - Transport Layer Security (TLS)," [Online]. Available: https://docs.stepfunc.io/dnp3/0.10.0/guide/docs/api/tls/?mc_cid=8d045fd4ed, 2022.

[62] Dong Jin, D. M. Nicol, and Guanhua Yan, "An event buffer flooding attack in dnp3 controlled scada systems," in *Proceedings of the 2011 Winter Simulation Conference (WSC)*, 2011, pp. 2614–2626.

[63] H. Zimmermann, "Osi reference model-the iso model of architecture for open systems interconnection," *IEEE Transactions on communications*, vol. 28, no. 4, pp. 425–432, 1980.

[64] A. Adib *et al.*, "On stability of voltage source inverters in weak grids," *IEEE Access*, vol. 6, pp. 4427–4439, 2018.

[65] Q. Peng, *et al.*, "On the stability of power electronics-dominated systems: Challenges and potential solutions," *IEEE Transactions on Industry Applications*, vol. 55, no. 6, pp. 7657–7670, 2019.

[66] A. Barua and M. A. A. Faruque, "Hall spoofing: A Non-Invasive DoS attack on Grid-Tied solar inverter," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 1273–1290.

[67] J. Ospina *et al.*, "Trustworthy cyberphysical energy systems: Time-delay attacks in a real-time co-simulation environment," in *Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy*, 2020.

[68] I. Zografopoulos, J. Ospina, and C. Konstantinou, "Special session: Harness the power of ders for secure communications in electric energy systems," in *2020 IEEE 38th International Conference on Computer Design (ICCD)*. IEEE, 2020, pp. 49–52.

[69] K. Stouffer *et al.*, "SP 800-82 Rev. 2 – Guide to industrial control systems (ICS) security," https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf, accessed: 2022-11-22.

[70] I. Zografopoulos and C. Konstantinou, "DERauth: a battery-based authentication scheme for distributed energy resources," in *IEEE Computer Society Symposium on VLSI (ISVLSI)*. IEEE, 2020, pp. 560–567.

[71] J. Ahn *et al.*, "An overview of quantum security for distributed energy resources," in *2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, 2021, pp. 1–7.

[72] P.-Y. Kong, "A review of quantum key distribution protocols in the perspective of smart grid communication security," *IEEE Systems Journal*, vol. 16, no. 1, pp. 41–54, 2022.

[73] Z. Tang *et al.*, "Quantum-secure microgrid," *IEEE Transactions on Power Systems*, vol. 36, no. 2, pp. 1250–1263, 2020.

[74] National Institute of Standards and Technology, "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," [Online]. Available: https://tinyurl.com/2p8jc8u9, 2022.

[75] R. Gottumukkala *et al.*, "Cyber-physical system security of vehicle charging stations," in *2019 IEEE Green Technologies Conference(GreenTech)*, 2019, pp. 1–5.

[76] A. Mitrokotsa, M. Rieback, and A. Tanenbaum, "Classification of rfid attacks," 01 2008, pp. 73–86.

[77] K. Haataja and P. Toivanen, "Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures," *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 384–392, 2010.

[78] M. A. Mustafa *et al.*, "Smart electric vehicle charging: Security analysis," in *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2013, pp. 1–6.

[79] C. Xenofontos *et al.*, "Consumer, commercial and industrial iot (in) security: attack taxonomy and case studies," *IEEE Internet of Things Journal*, 2021.

[80] S. Lakshminarayana *et al.*, "Load-altering attacks against power grids under covid-19 low-inertia conditions," 2022.

[81] I. Makhdoom *et al.*, "Anatomy of threats to the internet of things," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, 2019.

[82] J. Ospina *et al.*, "On the feasibility of load-changing attacks in power systems during the covid-19 pandemic," *IEEE Access*, vol. 9, 2020.

[83] B. Vignau *et al.*, "10 years of iot malware: A feature-based taxonomy," in *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2019, pp. 458–465.

[84] J. Stine, "Vestas data 'compromised' by cyber attack," https://reut.rs/3fYYJqB, 2021.

[85] R. J. Campbell, "Electric Grid Cybersecurity," https://fas.org/sgp/crs/homesec/R45312.pdf, 2018, accessed: 2020-08-30.

[86] J. Ye *et al.*, "A review of cyber-physical security for photovoltaic systems," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–1, 2021.

[87] Federal Energy Regulatory Commission Order No. 827, "Reactive Power Requirements for Non-Synchronous Generation," [Online]. Available: https://tinyurl.com/3vrspjj8, 2021.

[88] J. Staggs, D. Ferlemann, and S. Shenoi, "Wind farm security: attack surface, targets, scenarios and mitigation," *International Journal of Critical Infrastructure Protection*, vol. 17, pp. 3–14, 2017.

[89] T. S. Gopal *et al.*, "Mitigating mirai malware spreading in iot environment," in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2018, pp. 2226–2230.

[90] K. Lounis and M. Zulkernine, "Attacks and defenses in short-range wireless technologies for iot," *IEEE Access*, vol. 8, 2020.

[91] I. Zografopoulos *et al.*, "Security assessment and impact analysis of cyberattacks in integrated T&D power systems," in *Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2021, pp. 1–7.

[92] C. Konstantinou and O. M. Anubi, "Resilient cyber-physical energy systems using prior information based on gaussian process," *IEEE Transactions on Industrial Informatics*, vol. 18, pp. 2160–2168, 2021.

[93] Cybersecurity & Infrastructure Security Agency , "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa20-352a, 2021.

[94] S. Rath *et al.*, "Stealthy rootkit attacks on cyber-physical microgrids: Poster," in *Proceedings of the Twelfth ACM International Conference on Future Energy Systems*, 2021, pp. 294–295.

[95] S. Sahoo *et al.*, "On detection of false data in cooperative dc microgrids—a discordant element approach," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 6562–6571, 2020.

[96] S. Rath *et al.*, "Behind closed doors: Process-level rootkit attacks in cyber-physical microgrid systems," in *2022 IEEE Power & Energy Society General Meeting (PESGM)*, 2022, pp. 1–5.

[97] T. Bunsen *et al.*, "Global ev outlook 2018: Towards cross-modal electrification," 2018.

[98] S. Acharya *et al.*, "Cyber insurance against cyberattacks on electric vehicle charging stations," *IEEE Transactions on Smart Grid*, 2021.

[99] J. Antoun *et al.*, "A detailed security assessment of the ev charging ecosystem," *IEEE Network*, vol. 34, no. 3, pp. 200–207, 2020.

[100] D. Reeh, *et al.*, "Vulnerability analysis and risk assessment of ev charging system under cyber-physical threats," in *2019 IEEE Transportation Electrification Conference and Expo (ITEC)*, 2019, pp. 1–6.

[101] RECHARGE News, "New failure for flagship GE wind turbine as Cypress blade breaks in Germany," [Online]. Available: https://tinyurl.com/3pazjr7d, 2021.

[102] L. Paulsson, "Huge Vestas Wind Turbine Collapses in Northern Sweden in Rare Accident," [Online]. Available: https://www.insurancejournal.com/news/international/2020/11/23/591674.htm, 2021.

[103] J. Yan, C.-C. Liu, and M. Govindarasu, "Cyber intrusion of wind farm scada system and its impact analysis," in *2011 IEEE/PES Power Systems Conference and Exposition*. IEEE, 2011, pp. 1–6.

[104] Y. Zhang, Y. Xiang, and L. Wang, "Power system reliability assessment incorporating cyber attacks against wind farm energy management systems," *IEEE transactions on smart grid*, vol. 8, no. 5, 2016.

[105] Z. Ahmed *et al.*, "Protecting iots from mirai botnet attacks using blockchains," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2019, pp. 1–6.

[106] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against iot demand attacks," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019.

[107] C. Dang *et al.*, "Demand side load management for big industrial energy users under blockchain-based peer-to-peer electricity market," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6426–6435, 2019.

[108] E. Ronen *et al.*, "Iot goes nuclear: Creating a zigbee chain reaction," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017.

[109] I. Zografopoulos and C. Konstantinou, "Detection of malicious attacks in autonomous cyber-physical inverter-based microgrids," *IEEE Transactions on Industrial Informatics*, 2021.

[110] Y. Li *et al.*, "Active synchronous detection of deception attacks in microgrid control systems," *IEEE transactions on smart grid*, vol. 8, no. 1, pp. 373–375, 2016.

[111] A. Bidram *et al.*, "Resilient and cybersecure distributed control of inverter-based islanded microgrids," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 3881–3894, 2019.

[112] S. Sahoo, Y. Yang, and F. Blaabjerg, "Resilient synchronization strategy for ac microgrids under cyber attacks," *IEEE Transactions on Power Electronics*, vol. 36, no. 1, pp. 73–77, 2021.

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

[114] Z. Zhang and K.-T. Chau, "Pulse-width-modulation-based electromagnetic interference mitigation of bidirectional grid-connected converters for electric vehicles," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2803–2812, 2017.

[115] X. Zhou, J. Fan, and A. Q. Huang, "High-frequency resonance mitigation for plug-in hybrid electric vehicles' integration with a wide range of grid conditions," *IEEE Transactions on Power Electronics*, vol. 27, no. 11, pp. 4459–4471, 2012.

[116] S. Martinenas, K. Knezović, and M. Marinelli, "Management of power quality issues in low voltage networks using electric vehicles: Experimental validation," *IEEE Transactions on Power Delivery*, vol. 32, no. 2, pp. 971–979, 2017.

[117] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an internet of things environment," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1152–1167, 2017.

[118] S. Falas, C. Konstantinou, and M. K. Michael, "A hardware-based framework for secure firmware updates on embedded systems," in *2019 IFIP/IEEE 27th International Conference on Very Large Scale Integration (VLSI-SoC)*. IEEE, 2019, pp. 198–203.

[119] J. Kuusijärvi *et al.*, "Mitigating iot security threats with a trusted network element," in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2016, pp. 260–265.

[120] S. Jain *et al.*, "Blockchain and autonomous vehicles: Recent advances and future directions," *IEEE Access*, vol. 9, pp. 130 264–130 328, 2021.

[121] U.S. Department of Commerce, "Biden Administration Releases Implementation Strategy for $50 Billion CHIPS for America program," [Online]. Available: https://tinyurl.com/2p9xhw58, 2022.

[122] S. Paul *et al.*, "On vulnerability and resilience of cyber-physical power systems: A review," *IEEE Systems Journal*, vol. 16, no. 2, pp. 2367–2378, 2021.

[123] M. A. Haque *et al.*, "Cyber resilience framework for industrial control systems: concepts, metrics, and insights," in *2018 IEEE international conference on intelligence and security informatics (ISI)*. IEEE, 2018, pp. 25–30.

[124] N. Jacobs *et al.*, "Measurement and analysis of cyber resilience for control systems: An illustrative example," in *2018 Resilience Week (RWS)*. IEEE, 2018, pp. 38–46.

[125] V. Venkataramanan, A. Hahn, and A. Srivastava, "CP-SAM: Cyber-physical security assessment metric for monitoring microgrid resiliency," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, 2019.

[126] V. Venkataramanan, A. Srivastava, A. Hahn *et al.*, "CP-TRAM: Cyber-physical transmission resiliency assessment Metric," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5114–5123, 2020.

[127] A. Sedgewick *et al.*, "Framework for improving critical infrastructure cybersecurity, version 1.0," 2014.

[128] M. A. Haque *et al.*, "Cyber-physical systems resilience: Frameworks, metrics, complexities, challenges, and future directions," *Complexity Challenges in Cyber Physical Systems*, 2019.

[129] K. Tierney and M. Bruneau, "Conceptualizing and measuring resilience: A key to disaster loss reduction," *TR news*, no. 250, 2007.

[130] J. Ospina, V. Venkataramanan, and C. Konstantinou, "CPES-QSM: A Quantitative Method Towards the Secure Operation of Cyber-Physical Energy Systems," *IEEE Internet of Things Journal*, 2022.

[131] Electric Power Research Institute, "Creating Security Metrics for the Electric Sector, Version 2.0," [Online]. Available: https://www.epri.com/research/products/3002007886, 2017.

[132] Electric Power Research Institute, "EPRI OpenMetCalc User Guide: OpenMetCalc 3.0 User Manual," [Online]. Available: https://www.epri.com/research/programs/072143/results/3002019800, 2021.

[133] The Smart Grid Interoperability Panel, "NISTIR 7628 Rev. 1: Guidelines for Smart Grid Cybersecurity," https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final, 2014, accessed: 2022-11-27.

[134] Hawaiian Electric Company, Inc., "RULE NO. 14 – Service Connections and Facilities on Customer's Premises," https://tinyurl.com/43ptv9jy, accessed: 2022-11-27.

[135] C. Liu *et al.*, "Financially motivated fdi on sced in real-time electricity markets: Attacks and mitigation," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1949–1959, 2019.

[136] I. Zografopoulos *et al.*, "Mitigation of cyberattacks through battery storage for stable microgrid operation," in *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2022.

Ioannis Zografopoulos received his Ph.D. at the Computer, Electrical, and Mathematical Sciences and Engineering Division (CEMSE) of King Abdullah University of Science and Technology (KAUST) in 2023. Prior, he graduated with a B.Eng. and M.Eng. degrees in Computer, Communications, and Network Engineering, and an M.Sc. degree in Electrical and Computer Engineering from the University of Thessaly, Volos, Greece, in 2014 and 2015, respectively. His research interests include cyber-physical systems security, with an emphasis on embedded systems for industrial, distributed energy, and power grid applications. He is an IEEE and IEEE PES graduate student member, a member of IET, and has served as a reviewer for the IEEE Transactions on Power Systems, Transactions on Industrial Electronics, IEEE Transactions on Transportation Electrification, IEEE Internet of Things (IoT), and other IEEE and ACM conferences and journals.

Nikos D. Hatziargyriou (Life Fellow, IEEE) has been with the National Technical University of Athens, Athens, Greece, since 1984, a Professor of power systems, since 1995, and Professor Emeritus, since 2022. He is currently a part-time Professor with the University of Vaasa, Vaasa, Finland. He has more than 10 years of industrial experience as the Chairman and CEO with the Hellenic Distribution Network Operator, and Executive Vice-Chair and Deputy CEO with the Public Power Corporation, responsible for the Transmission and Distribution Divisions. He has participated in more than 60 R&D projects funded by the EU Commission, electric utilities and industry for fundamental research and practical applications. He has authored or co-authored more than 300 journal publications and 600 conference proceedings papers. He was the Chair and Vice-Chair of ETIP-SNET. He is the past EiC of IEEE TRANSACTIONS ON POWER SYSTEMS. He is an EiC-at-Large for IEEE PES TRANSACTIONS. He is included in the 2016, 2017 and 2019 Thomson Reuters lists of top 1% most cited researchers. He was the 2020 Globe Energy Prize laureate, recipient of the 2017 IEEE/PES Prabha S. Kundur Power System Dynamics and Control Award and 2023 IEEE Herman Halperin Electric Transmission and Distribution Award.

Charalambos Konstantinou (SM'20) received the M.Eng. degree in electrical and computer engineering from the National Technical University of Athens (NTUA), Greece, in 2012, and the Ph.D. degree in electrical engineering from New York University (NYU), NY, USA, in 2018. He is currently an Assistant Professor of Electrical and Computer Engineering (ECE) and an Affiliate Professor of Computer Science (CS) with the Computer, Electrical and Mathematical Science and Engineering Division (CEMSE), King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia. He is the Principal Investigator of the Secure Next Generation Resilient Systems Laboratory (sentry.kaust.edu.sa) and a member of the Resilient Computing and Cybersecurity Center (RC3), KAUST. His research interests include critical infrastructures security and resilience with special focus on smart grid technologies, renewable energy integration, and real-time simulation. He is the Chair of the IEEE Task Force on Resilient and Secure Large-Scale Energy Internet Systems and the Co-Chair of the IEEE Task Force on Cyber-Physical Interdependence for Power System Operation and Control. He is a member of ACM and an ACM Distinguished Speaker (2021–2024). Prof. Konstantinou is an Associate Editor of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS.