Cyber resilience of power electronics-enabled power systems: A review

Article *in* Renewable and Sustainable Energy Reviews · January 2024

DOI: 10.1016/j.rser.2023.114036

4 authors, including:

Jiazuo Hou
National University of Singapore
15 PUBLICATIONS **55** CITATIONS

SEE PROFILE

Shunbo Lei
University of Michigan
67 PUBLICATIONS **2,312** CITATIONS

SEE PROFILE

Yunhe Hou
The University of Hong Kong
227 PUBLICATIONS **5,909** CITATIONS

SEE PROFILE

Cyber Resilience of Power Electronics-Enabled Power Systems: A Review

Jiazuo Hou[a], Chenxi Hu[a], Shunbo Lei[b], Yunhe Hou[a,*]

[a] *Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong, China*
[b] *School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen, Guangdong 518172, China*

Abstract

The demand for carbon neutrality leads to the transition from traditional synchronous generator-based power systems to power electronics-enabled power systems. The controllability and observability of power electronics devices are achieved by underlying metering and communication infrastructures, which are vulnerable to cyber-attacks. This review comprehensively investigates the cyber resilience of power electronics-enabled power systems from three aspects, i.e., before, during, and after cyber-attack events. Specifically, the cyber resilience of multiple power electronics devices in power generation (photovoltaic and wind), power transmission (high-voltage direct-current), power prosumption (electric vehicle, smart building, microgrid), power storage, and grid-tied converters, are addressed, respectively. In addition, this review thoroughly investigates the representative cyber-attack events, cyber-defense threats, cybersecurity regulations, and graphical cyber-physical architectures of the power electronics-enabled power system. As a result, this review

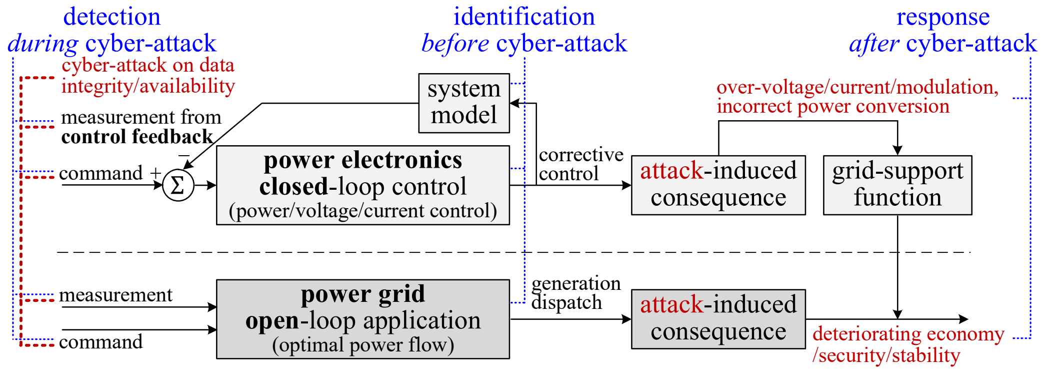
[*] Corresponding author
Email address: yhhou@eee.hku.hk (Yunhe Hou)

proposes a general cybersecurity paradigm of power electronics closed-loop controllers. Therein, the cyber timescale, stealthiness, and threat between power electronics closed-loop controllers and power grid open-loop applications are investigated, respectively.

Highlights

- Cyber resilience of power electronics devices before, during, and after cyber events.
- A general cybersecurity paradigm of power electronics closed-loop controllers.
- Cyber events, threats, and regulations of power electronics-enabled power systems.
- Graphical cyber-physical architectures of multiple power electronics devices.

Graphical abstract



Keywords

Cyber resilience, cyber-attack event, cyber-defense threat, cybersecurity regulation, power electronics device, power electronics-enable power system.

Word count

8537 words.

Abbreviations

AC	alternating current
BACnet	Building Automation and Control network
DC	direct current
DFIG	doubly-fed induction generator
DoE	Department of Energy
DoS	denial of service
FDI	false data injection
HVAC	heating, ventilation, and air-conditioning
HVDC	high-voltage direct-current
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LCC	line-commutated converter

MMC	modular-multilevel converter
MPPT	maximum power point tracking
NERC	North American Electric Reliability Corporation
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
OPF	optimal power flow
PMSG	permanent magnet synchronous generator
PV	photovoltaic
SAE	Society of Automotive Engineers
SG	synchronous generator
VSC	voltage-sourced converter

1. Introduction

1.1. Cyber vulnerability of the power electronics-enabled power system

In response to global warming and climate crisis, many countries have proposed roadmaps to achieve carbon neutrality [1]. As shown in Fig. 1, the demand for net zero, as well as better grid flexibility, leads to the increasing integration of power electronics devices [2] in different parts of a power system, including but not limited to power generation (e.g., wind, photovoltaic), power transmission (e.g., high-voltage direct-current system), power prosumption (e.g., electric vehicle, smart building, and microgrid), and power storage (e.g., energy storage system). This leads to a transition from a traditional synchronous generator (SG) based power system to a power electronics-enabled power system [3].

As a result, the power electronics-enabled power system is enabled with higher controllability and observability [4]. This is achieved via miscellaneous power electronics controllers that heavily rely on related metering and communication infrastructure to collect measurement data from sensors, download command data to actuators, and exchange necessary information with other power electronics devices [5]. The underlying cyber layer, unfortunately, introduces additional access points, i.e., cyber threats, which are attractive for cyber-attackers and troublesome for system operators [6].

Hence, recent years have witnessed increasing reports of cyber-attack events, which grow by nearly 2000% from 2006 to 2019 [7]. Specifically,

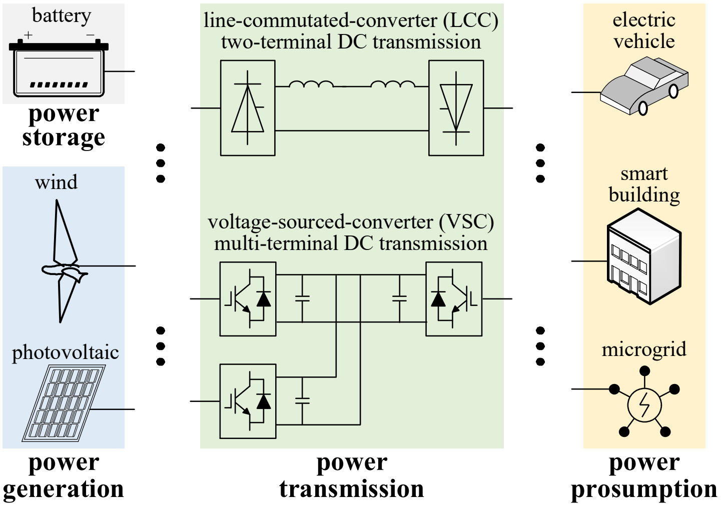


Figure 1: A power electronics-enabled power system with power electronics devices in power generation, power transmission, power prosumption, and power storage.

the representative cyber-attack events on each power electronics device are illustrated in Table 1, which indicates that the current cyber-physical power electronics-enabled power system is rather vulnerable to cyber-attacks [8]. Therefore, as depicted in Fig. 2, different cybersecurity regulations and roadmaps are proposed for not only power systems (e.g., IEC 62351 [9], IEC 62443 [10], NIST 7628 [11]) but also power electronics devices [12], including photovoltaic [13], wind [14], distributed energy resource [15], high-voltage direct-current system [16], electric vehicle [17], smart building [18], microgrid [19], energy storage system [20], etc. The detailed cybersecurity regulations are illustrated in Table A.1 and Table A.2 in Appendix A. It is observed that previous studies pay much attention to the cybersecurity of industrial and power systems [21], while cybersecurity for specific power electronics devices has been attracting more and more attention for recent five years. This indicates the emerging need for enhancing the cyber resilience of the power electronics-enabled power system against cyber-attack events [5].

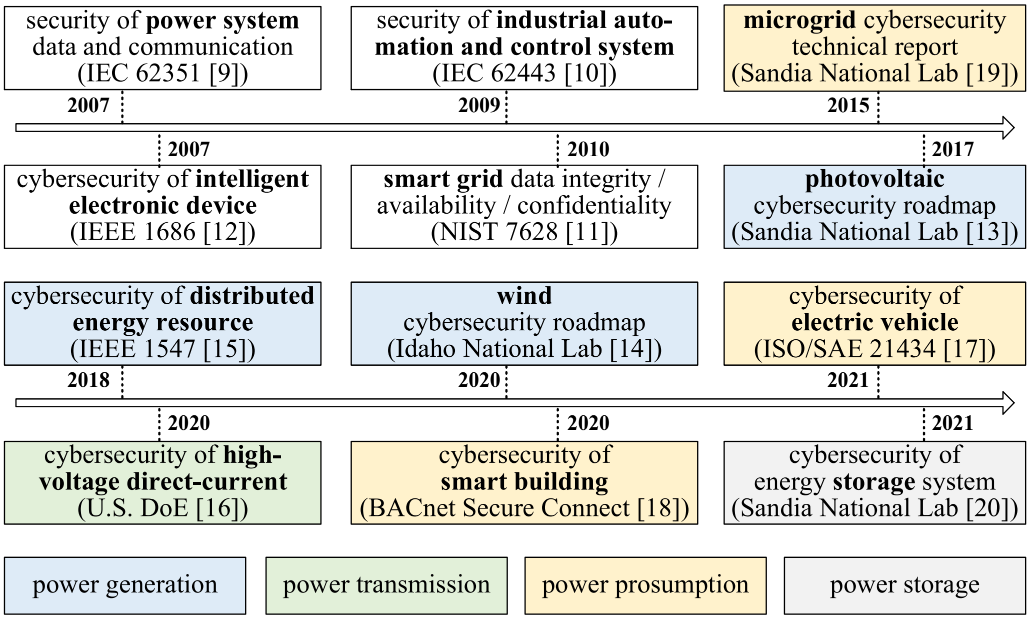

security of power system data and communication (IEC 62351 [9])
security of industrial automation and control system (IEC 62443 [10])
microgrid cybersecurity technical report (Sandia National Lab [19])
2007
2009
2015
2007
2010
2017
cybersecurity of intelligent electronic device (IEEE 1686 [12])
smart grid data integrity / availability / confidentiality (NIST 7628 [11])
photovoltaic cybersecurity roadmap (Sandia National Lab [13])
cybersecurity of distributed energy resource (IEEE 1547 [15])
wind cybersecurity roadmap (Idaho National Lab [14])
cybersecurity of electric vehicle (ISO/SAE 21434 [17])
2018
2020
2021
2020
2020
2021
cybersecurity of high-voltage direct-current (U.S. DoE [16])
cybersecurity of smart building (BACnet Secure Connect [18])
cybersecurity of energy storage system (Sandia National Lab [20])
power generation
power transmission
power prosumption
power storage

Figure 2: A timeline of representative regulations and roadmaps of power systems and power electronics devices. BACnet: Building Autmoation and Control network. DoE: Department of Energy. IEC: International Organization for Standardization. NIST: National Institute of Standards and Technology. SAE: Society of Automotive Engineers.

Table 1: Representative cyber-attack events on power electronics devices in power systems

Category	Device	Description	Location	Time	Study
Generation	wind	A wind operator's control was ceased by a cyber-attack over around 500 MW of wind turbines.	U.S.	2019	[14]
	photovoltaic	A 106 MW PV project was compromised by a denial-of-service cyber-attack.	U.S.	2021	[22]
Transmission	high-voltage direct-current	ABB U.S. Corporate Research Center demonstrated negative impacts of FDI attacks targeting HVDC stations.	U.S.	2019	[23]
Prosumption	electric vehicle	A Jeep Cherokee was remotely controlled and its acceleration and brakes were shutted down.	U.S.	2015	[24]
		Tesla's steering system was remotely controlled and its auto-wiper function was disturbed.	China	2019	[25]
	smart building	The building management system of Google Australia Office was hacked.	Australia	2013	[26]
		A top retailer was hacked, leading to the exposure of about 40 million debit and credit card accounts.	U.S.	2019	[27]
	microgrid	Cyber attacks against the Ukrainian power grid resulted in approximately 225,000 customers without power supply.	Ukraine	2015	[28]
Storage		The smart battery controller of a MacBook was hacked and its battery data was modified.	U.S.	2011	[29]

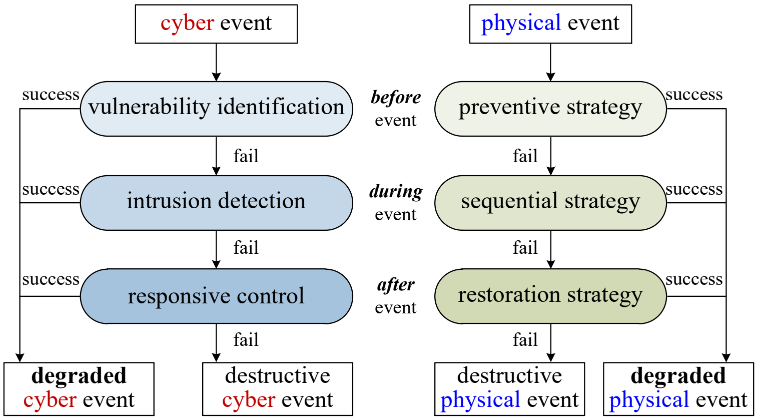


Figure 3: Cyber or physical resilience before, during, and after a cyber or physical event.

1.2. Cyber resilience of the power electronics-enabled power system

Generally, the resilience of a system is defined as the ability to "anticipate, absorb, adapt to and/or rapidly recover from a disruptive event" [30]. For the disruptive physical events (e.g., hurricane, flood, sandstorm, etc.) on a power system, the physical resilience enhancement strategies are usually divided into three stages in Fig. 3 [31], i.e., 1) resilience assessment and/or resource pre-allocation before the physical event; 2) sequential response and/or attack-defense game during the physical event; 3) system restoration after the physical event. Similarly, the cyber resilience enhancement strategies of the power electronics-enabled power system can be divided into three stages, i.e., identification, detection, and response, which are widely accepted by the power industry [14, 13] and academia [31, 32].

As shown in Fig. 3 [13, 31], before the cyber-attack event, the cyber defenders focus on finding cyber threats, identifying cyber-attack paths, and evaluating the impacts. During the cyber-attack event, the cyber defenders concentrate on the cyber-attack detection using either model-based methods or data-driven methods. Both the identification strategies and detection strategies focus on avoiding the successful connection between cyber-attacks and power grids. After the cyber-attack event, the cyber defenders aim to effectively respond and mitigate the cyber-attack using cyber resilient strategies.

1.3. Related reviews regarding cyber resilience of power electronics-enabled power systems

The importance of power system physical resilience has been well identified. For instance, Ahmadi et al. [33] present a review of the energy system physical resilience from analytical, technical, and mathematical viewpoints. Moreover, Younesi et al. [34] investigate the resources and methods to evaluate and improve the power system physical resilience from the perspective of smart grids. Apart from physical resilience, the cyber resilience of traditional SG-based power systems is another important topic. For example, Xu et al. [31] provide a review of the cyber-physical resilience-oriented techniques based on a general system theory. Furthermore, a comprehensive review of energy system cyber and physical resilience is presented with a detailed landscape of threats and countermeasures [35].

Nevertheless, studies on the cyber resilience of power electronics devices inside a power system are limited. The pioneering work [5], which is under a committee from the IEEE Power Electronics Society, investigates the need for cybersecurity solutions to the power electronic systems from both hardware and software mechanisms. As shown in Table 2, most of the previous efforts have been focused on the cyber resilience of individual power electronics devices.

First, for the power electronics devices in power generation, the U.S. Department of Energy publish several roadmaps regarding the cyber resilience of the photovoltaic system [13, 36] and the wind system [14, 37]. Moreover, Ye et al. [38] address the cyber resilience of the photovoltaic system from a hardware, firmware, communication, and network perspective. Furthermore, Zografopoulos et al. [39] investigate cyber-attacks targeting the autonomous capabilities and ancillary services of distributed energy resources (DER). In addition, Tuyen et al. [40] illustrate the cyber vulnerabilities of grid-supportive services of DER. Second, for the power electronics devices in power transmission, a technical report [16] is published to address the threat modeling, intrusion detection, and hardware-in-the-loop test-bed of the cybersecurity of the high-voltage direct-current transmission systems. Third, for the power electronics devices in power prosumption, the cyber resilience of the charging infrastructures [41, 42] and connected network [43] of electric vehicles are investigated. Moreover, Li et al. [44] address the cyber vulnerabilities of building automation systems at management, automation, and field level. Furthermore, Gaggero et al. [45] and Jmail et al. [46] identify the cyber vulnerabilities and recent advancements of microgrids. Fourth, for the power electronics devices in power storage, Trevizan et al. [47] and Johnson et al. [48] investigate the attack vectors, protective measures for grid-connected battery energy storage systems and corresponding grid-support applications. Finally, the cyber resilience of grid-tied converters is comprehensively investigated by identifying the potential cyber vulnerabilities from device/grid level [49] and control/cyber layer [50].

Table 2: Comparison of related studies regarding cyber resilience of power electronics devices in power systems

studies	**physical resilience**	**cyber resilience**					
		power generation	power transmission	power prosumption	power storage	power electronics converter	cybersecurity paradigm shift
[33, 34]	✓	-	-	-	-	-	-
[36, 38], [14, 37], [39, 40]	-	photovoltaic, wind, DER	-	-	-	-	-
[16]	-	-	HVDC	-	-	-	-
[42, 43], [44], [45, 46]	-	-	-	electric vehicle, smart building, microgrid	-	-	-
[47, 48]	-	-	-	-	battery energy storage system	-	-
[49, 50]	-	-	-	-	-	grid-tied converter	-
this review	-	✓	✓	✓	✓	✓	✓

However, few previous efforts focus on the cyber resilience of a power electronics-enabled power system with multiple power electronics devices (in power generation, power transmission, power prosumption, and power storage) from all three aspects, i.e., before, during, and after cyber-attack events. More importantly, the general cybersecurity paradigm of power electronics controllers, which is experiencing a significant paradigm shift from the cybersecurity paradigm of power grid applications, is still not investigated sufficiently.

Therefore, to investigate the cyber resilience of a power electronics-enabled power system, three different research fields need to be addressed, including the

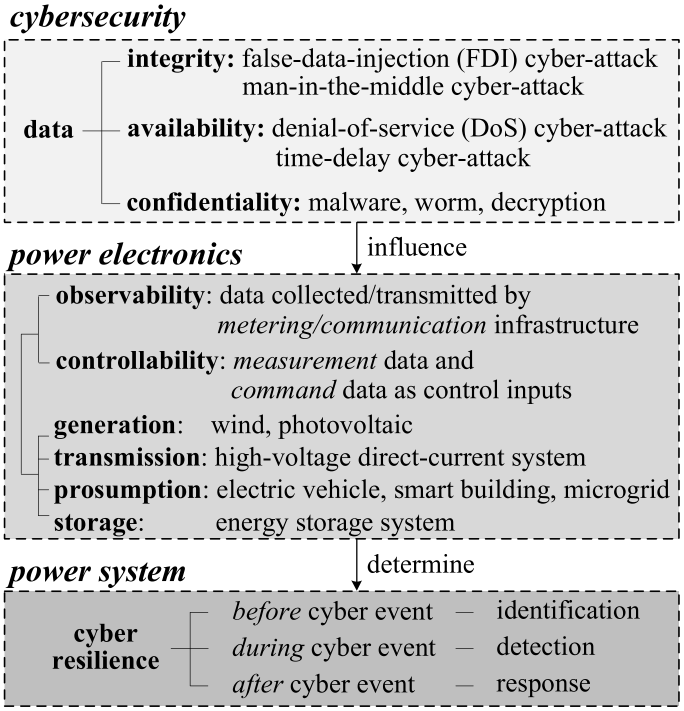

cybersecurity
data
integrity: false-data-injection (FDI) cyber-attack
man-in-the-middle cyber-attack
availability: denial-of-service (DoS) cyber-attack
time-delay cyber-attack
confidentiality: malware, worm, decryption
influence
power electronics
observability: data collected/transmitted by
metering/communication infrastructure
controllability: measurement data and
command data as control inputs
generation: wind, photovoltaic
transmission: high-voltage direct-current system
prosumption: electric vehicle, smart building, microgrid
storage: energy storage system
determine
power system
cyber resilience
before cyber event – identification
during cyber event – detection
after cyber event – response

Figure 4: Three interdependent research fields in investigating the cyber resilience of a power electronics-enabled power system.

cybersecurity, the power electronics, and the power system, whose interactions are illustrated in Fig. 4. First, the resilience of a power system before, during, and after a cyber-attack event is significantly determined by the performance of the interconnected power electronics devices, which are geographically widespread in power generation, power transmission, power prosumption, and power storage. Then, the controllability and observability of each power electronics device depend on the measurement and command data, which are collected and transmitted via underlying metering and communication infrastructure, respectively. In addition, the measurement and command data could be compromised by cyber-attacks in the sense of data integrity (e.g., the false-data-injection cyber-attack), data availability (e.g., the denial-of-service cyber-attack), and data confidentiality (e.g., malware).

The contributions of this review are summarized as follows. First, from the viewpoints before, during, and after cyber-attack events, this review comprehensively investigates the cyber resilience of power electronics-enabled power systems. Specifically, the cyber resilience of multiple power electronics devices in power generation (photovoltaic and wind), power transmission (high-voltage direct-current), power prosumption (electric vehicle, smart building, microgrid), power storage, and grid-tied converters, are addressed, respectively. In addition, this review thoroughly investigates the representative cyber-attack events, cyber-defense threats, cybersecurity regulations, and graphical cyber-physical architectures of the power electronics-enabled power system. As a result, this review proposes a general cybersecurity paradigm of power electronics closed-loop controllers. Therein, the cyber timescale, stealthiness, and threat between power electronics closed-loop controllers and power grid open-loop applications are investigated, respectively.

2. Cyber resilience of grid-tied converters

Typically, the DC/AC (or AC/DC) power electronics converters can be divided into two main types, i.e., the line-commutated-converters (LCC) and the voltage-sourced-converters (VSC). The LCC is usually applied for two-terminal HVDC transmission systems, which will be illustrated in Section 4. The VSC, including the modular-multilevel-converters (MMC), is the widely used energy conversion interface that bridges the power grid and the interconnected power electronics devices, which include the converter-based resources such as the wind [14], photovoltaic [13], HVDC [16], electric vehicle [41], smart building [51], microgrid [52], energy storage system [20], etc.

As shown in Fig. 5, the grid-tied converter, which is a cyber-physical system, is operated in a hierarchical control and communication architecture with multiple control in multiple levels. First, according to the command

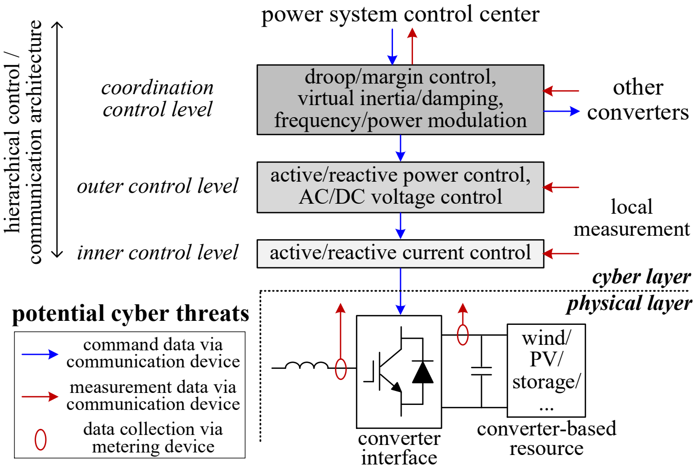

power system control center
hierarchical control / communication architecture
coordination control level
droop/margin control, virtual inertia/damping, frequency/power modulation
other converters
outer control level
active/reactive power control, AC/DC voltage control
local measurement
inner control level
active/reactive current control
cyber layer
physical layer
potential cyber threats
command data via communication device
measurement data via communication device
data collection via metering device
wind/ PV/ storage/ ...
converter interface
converter-based resource

Figure 5: Control and communication architecture of a grid-tied converter.

from the control center and other converters, the coordination control level (e.g., the virtual inertia/damping control [53], frequency/power modulation control [54], droop/margin control [55]) provides references for the outer control level. Then, according to the received command and the collected measurement, the outer control level (e.g., active/reactive power control and AC/DC voltage control [56]) provides references for the inner control level. Finally, according to the received command and the collected measurement, the inner control level (e.g., active/reactive current control) provides references for the switching devices.

The cyber vulnerabilities of each control level are different from each other due to different control timescales, different metering and communication devices. However, all the collected measurement data and the transmitted command data in different control levels could be potential cyber threats, including [38]: 1) remote or owner access via software update or user interface; 2) access via flash drives or local area network; 3) firmware modification and malware injection; 4) reverse engineering physical access. Specifically, the cyber resilience of the grid-tied converter before, during, and after a cyber-attack event is investigated as follows.

2.1. Before a cyber-attack event

For cyber-attack impacts on local controllers, Zografopoulos et al. [57] evaluate the impacts of firmware cyber-attacks on the maximum power point tracking (MPPT) controller of a grid-tied solar inverter. Moreover, for cyber-attack impacts on grid-support functions, Sahoo et al. [50] evaluate various cyber-attacks on the VSC grid-supportive services, including frequency response control, wide-area damping control, etc. Similarly, Barua et al. [58]

demonstrate that a stealthy non-invasive DoS cyber-attack could spoof the Hall sensor of a grid-tied solar inverter to perturb grid voltage, frequency, active and reactive power.

2.2. During a cyber-attack event

For model-based cyber-attack detection, Burgos-Mellado et al. [59] propose a Kalman filter-based method to detect the FDI cyber-attacks on the voltage sensor measurement of sub-modules inside an MMC. Moreover, Zhang et al. [60] present a model-based detection method to identify cyber-attacks on the interleaved active neutral point clamped PV converter based on a Kalman filter and state-space model. In addition, for data-driven cyber-attack detection, Li et al. [61] propose a multi-layer long short-term memory network-based detection algorithm against data integrity cyber-attacks on dc-dc converters and dc-ac converters of PV systems.

2.3. After a cyber-attack event

Wang et al. [62] propose a distributed cyber-resilient cooperative control for bidirectional interlinking converters against FDI cyber-attacks. Similarly, Sahoo et al. [63] present an adaptive cyber-resilient controller for the synchronization of multiple cooperative grid-forming converters against FDI cyber-attacks. In addition, using a digital model predictive controller and an analog proportional integral controller, Chen et al. [64] propose a parallel control framework against cyber-attacks on power electronics converters.

Remark: As a general energy conversion interface between power electronics devices and a power grid, the converter itself is also part of the interconnected power electronics devices. Cyber threats exist in each control level of the hierarchical communication architecture with different control timescales. In this regard, the power electronics converter could be prior target for cyber-attackers from either hardware modifications or software injections.

3. Cyber resilience of power generation

This section investigates the cyber resilience of two typical power electronics-based devices in power generation, i.e., photovoltaic and wind generation systems.

3.1. Photovoltaic

To reach the goal of carbon neutrality, the penetration rate of renewable energy sources is increasing at an incredible speed. In 2022, PV generation has increased by 270 TWh (26ĉompared with 2021), reaching around 1300 TWh [65]. It is estimated that solar energy can serve more than 40% of the electricity demand in the U.S [66].

As shown in Fig. 6 [67], the PV system, which is a cyber-physical system, is vulnerable to cyber-attacks on both the DC/DC converter and the DC/AC converter. For instance, in 2019, a 106 MW PV project is compromised in California, U.S., due to a DoS cyber-attack on the firewall [22]. Thus, as shown in Table 3, the cybersecurity of the PV system has been attracting attention from national laboratories and universities for recent five years. The cyber treats of a PV system include but are not limited to [13] the lack of cybersecurity investment by industry, the insufficient information sharing of cyber vulnerabilities and incidents. Specifically, the cyber resilience of a PV system before and during a cyber-attack event is investigated as follows.

3.1.1. Before a cyber-attack event

Using Markov-based state transition rules, Liu et al. [70] propose a risk assessment method to evaluate the cybersecurity of PV-based microgrids when PV control systems are hacked. Moreover, Teymouri et al. [71] evaluate the economic impacts of cyber-attack on the reactive power control loop of a grid-connected PV system.

3.1.2. During a cyber-attack event

For model-based cyber-attack detection, Isozaki et al. [72] propose a four-step rule-based detection algorithm against cyber-attacks that falsify the voltage control measurement and could lead to voltage violation and output power loss. In addition, Ibrahim et al. [73] present an active detection method to detect cyber-attacks on sensor measurements of grid-tied PV systems by introducing a private watermarking signal.

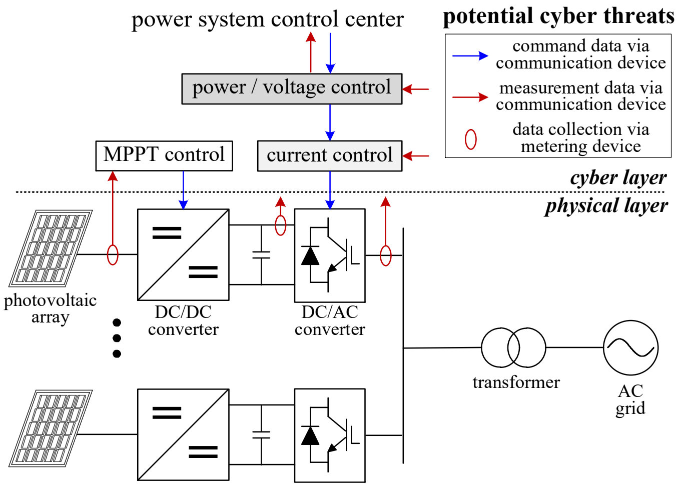


Figure 6: Control and communication architecture of a typical photovoltaic system. MPPT: maximum power point tracking.

Table 3: Technical reports and reviews of PV cybersecurity

theme	institute	year
DER cybersecurity [68]	Sandia National Laboratory	2017
cybersecurity of general PV systems (roadmap) [13]		2017
cybersecurity of general PV systems (final report) [36]		2019
cybersecurity of distributed PV [69]		2019
cybersecurity of PV plant operation [22]	National Renewable Energy Laboratory	2021
review of PV cyber-physical security [38]	University of Georgia	2021

For data-driven cyber-attack detection, Guo et al. [67] propose a deep-learning-based cyber-attack detection method for power electronics converter-enabled PV farms to distinguish between cyber-attacks, normal conditions, and faults. Moreover, Li et al. [74] present a waveform data-based signal processing and online statistics associated method to detect cyber and physical attacks on PV-interconnected distribution power grids. Furthermore, [75] proposes a data-driven cyber-attack detection method for PV systems using a transfer learning method and a convolutional neural network model. In addition, [76] compares the performances of multiple data-drive detection methods (e.g., artificial neural network and long short-term memory) that use micro-phasor measurement units to detect the cyber-attacks on PV systems.

3.2. Wind Generation

To achieve net-zero emissions in the future, wind generation keeps a fast-growing trend in the past years [77]. The new capacity installed of global wind energy increased by 78 GW and 265 TWh, reaching up to 906 GW and 2100 TWh in total [78, 79].

As shown in Fig. 7 [14], the wind generation, including the doubly-fed induction generator (DFIG) type and the permanent magnet synchronous generator (PMSG) type, is a cyber-physical system, which could be compromised by multiple cyber threats: 1) the trend of digitalization and coordination control of wind farms [80]; 2) the various communication protocols from different interests [37]; 3) the lack of wind-specific cybersecurity standards and products [81]; 4) the multiple parties involved in the wind plant lifecycle [14].

As a result, the consequences of cyber-attacks on wind generation could

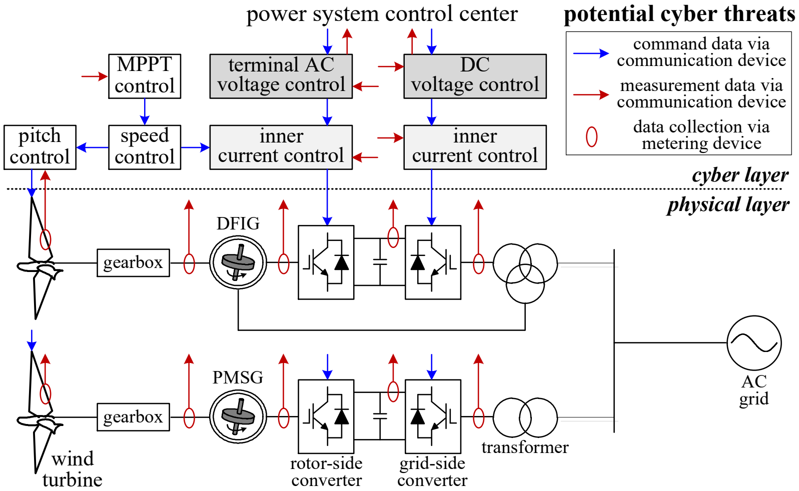


Figure 7: Control and communication architecture of the doubly-fed induction generator (DFIG) wind generation and the permanent magnet synchronous generator (PMSG) wind generation. MPPT: maximum power point tracking.

be the wind turbine manipulation [14], the wind farm disruption, and the substation damage [82]. For instance, a wind operator's control was ceased by a cyber-attack over around 500 MW of wind turbines in Salt Lake City, U.S. in 2019 [14]. Hence, both academia and industry have been devoted to wind cyber resilience in recent years. Idaho National Laboratory has published a cybersecurity roadmap for bulk wind projects [14] and a cybersecurity guide for distributed wind [37]. Therein, the cyber resilience enhancement strategies for wind energy are divided into four parts, i.e., wind cyber-culture development, identification, detection, and response [14]. Moreover, a research project under General Electric Global Research and the U.S. Department of Energy focuses to accommodate and respond to cyber-attacks on wind generation by proposing a novel classification and risk prioritization structure [83]. In addition, technical companies, e.g., General Electric, provide a set of professional solutions and services to assess, harden, and maintain the cybersecurity of wind farms [81]. Detailed studies regarding the cyber resilience of wind energy are investigated as follows.

3.2.1. Before a cyber-attack event

For the wind farm, Yan et al. [84] identify the cyber vulnerabilities of a wind farm supervisory control and data acquisition system and its impact on power system dynamics. Moreover, Zhang et al. [85] identify critical cyber-attack scenarios of an integrated wind farm energy management system using Bayesian attack graph models. Furthermore, Wu et al. [86] evaluate the impact of wind farms' cybersecurity by modelling cyber-attacks on instantaneous failure and longtime fatigue of wind turbines.

For wind turbines, [87] and [88] identify the cyber vulnerabilities of two different wind turbines. For wind grid-support functions, Johnson et al. [89] evaluate the risks of cyber-attacks on the grid-support functions, including frequency ride-through trip, voltage ride-through trip, soft-start ramp, frequency-watt, and voltage-watt functions, etc. For wind-integrated power systems, Liu et al. [90] propose a cybersecurity assessment approach using deep reinforcement learning and an adapted Common Vulnerability Scoring System. For wind power forecasting, Zhang et al. [91] quantify the robustness of wind power forecasting against FDI cyber-attack using the Monte Carlo method.

3.2.2. During a cyber-attack event

For data-driven cyber-attack detection, Bi et al. [92] propose a meta-learning-based detection network to mitigate profit-oriented FDI cyber-attack against wind farms. Moreover, Marino et al. [93] introduce a fully virtualized testbed for data-driven anomaly detection systems in a wind-powered grid.

3.2.3. After a cyber-attack event

Amini et al. [94] propose an observer-based cyber resilient control framework for a DFIG-based wind park against DoS and/or deception cyber-attacks that attempt to destabilize the wind park from a sub-synchronous perspective. In addition, Ghafouri et al. [95] present a robust static-output-feedback controller for a DFIG-based wind park against sub-synchronous interaction-related cyber-attacks.

Remark: Typically, the PV system operates with a DC/DC converter and a DC/AC converter, while the wind system operates with a rotor-side AC/DC converter and a grid-side DC/AC converter. Although the control strategies are different, both the PV system and the wind system are intrinsically cyber-physical systems that are vulnerable to potential cyber-attacks. More attention should be paid to the cybersecurity of not only PV arrays and wind turbines but also the interdependent converters, including DC/DC, DC/AC, and AC/DC.

4. Cyber resilience of HVDC transmission

As a critical infrastructure to meet the demand of long-distance bulk power transmission, the HVDC transmission system plays an important role in determining the secure operation of the whole power system. The total HVDC transmission capacity is expected to achieve 400 GW in 2022, some of which even exceeds 10 GW in China [96]. The HVDC transmission system market has more than 12.61 billion U.S. dollars market size in 2023 and this value is expected to be 19.65 billion U.S. dollars in 2028 [97].

There are mainly two types of HVDC systems [98], i.e., the LCC HVDC transmission system that is suitable for two-terminal applications, and the VSC transmission system that is suitable for multi-terminal applications. Since the thyristor has a relative higher voltage level and power level than the insulated gate bipolar translator currently, the LCC HVDC still plays a more predominant role in numbers than VSC HVDC in ultra- and extra- HVDC transmission projects [99]. However, since the VSC HVDC system is capable of simultaneously controlling both the active power and reactive power, it is a more promising technology than the LCC HVDC system [100]. Hence, both the two kinds of HVDC systems are of great importance [16], [101].

According to IEC 60919 [102], the control and communication architecture of a two-terminal LCC HVDC system is depicted in Fig. 8. Therein, the inter-station control (e.g., the current margin control [102]) receives the command from the control center and coordinates the control references in both the rectifier station and inverter station. Then, the intra-station control inside each HVDC station (e.g., the DC current control in the rectifier station and the DC voltage control in the inverter station) provides the firing angle for the thyristors.

By comparison, according to IEC 60543 [103], the control and communication architecture of a multi-terminal VSC HVDC system is depicted in Fig. 9. Therein, the intra-station control (e.g., the outer power/voltage control and inner current control) provides references for the IGBTs according to the received command and the collected measurement. In addition, the inter-station control (e.g., the leader/follower control [104], the voltage droop control [55], the voltage margin control [104]) globally coordinates multiple VSC stations with real-time information exchange.

In other words, both the LCC and VSC HVDC system are cyber-physical

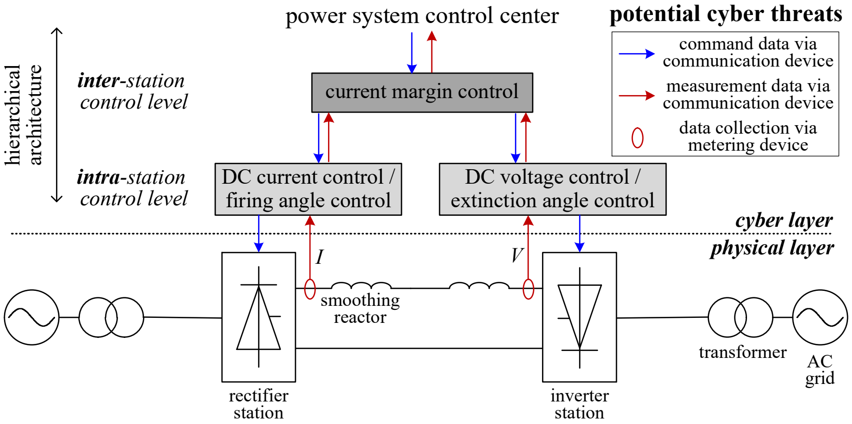

power system control center
potential cyber threats
command data via communication device
measurement data via communication device
data collection via metering device
hierarchical architecture
inter-station control level
intra-station control level
current margin control
DC current control / firing angle control
DC voltage control / extinction angle control
cyber layer
physical layer
I
V
smoothing reactor
rectifier station
inverter station
transformer
AC grid

Figure 8: Control and communication architecture of a two-terminal LCC HVDC system.

systems, which could be vulnerable to cyber threats, including: 1) the increasing access points due to the trend to digital HVDC stations [105]; 2) the insufficient computing resources to support cybersecurity capabilities [101]; 3) the geographically widespread and publicly accessible HVDC stations [16]; 4) the trade-off between cybersecurity capability and real-time emergency response [101]. Therefore, the cybersecurity of the HVDC transmission system has been receiving attention from both academia [101] and industry, including Texas Instruments [106], Hitachi Energy [107], and Siemens Energy [108]. Detailed studies regarding the cyber resilience of the HVDC system are investigated as follows.

4.1. Before a cyber-attack event

Using a structured pseudospectrum and a vertical search method, Ding et al. [109] evaluate the impacts of cyber-attacks on the small-signal stability margin of a two-terminal MMC HVDC system. Moreover, Zhao et al. [110]

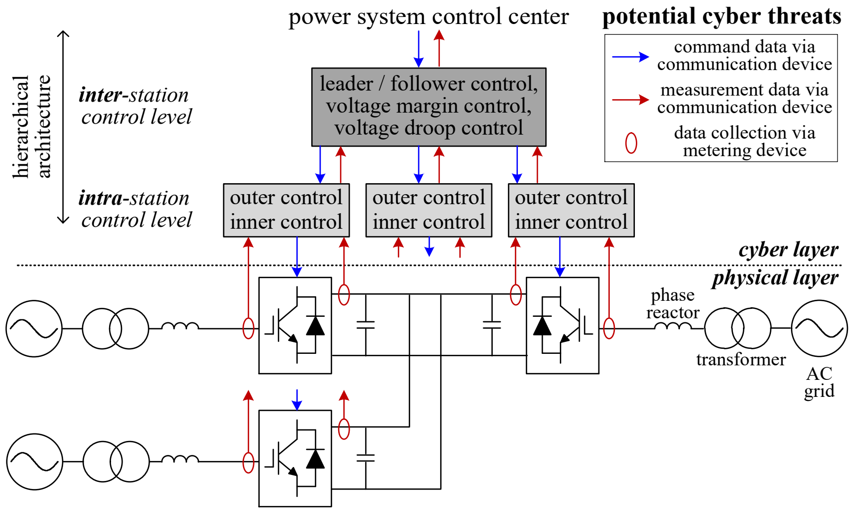

power system control center
potential cyber threats
command data via communication device
measurement data via communication device
data collection via metering device
hierarchical architecture
inter-station control level
intra-station control level
leader / follower control, voltage margin control, voltage droop control
outer control
inner control
outer control
inner control
outer control
inner control
cyber layer
physical layer
phase reactor
transformer
AC grid

Figure 9: Control and communication architecture of a multi-terminal VSC HVDC system.

propose a novel index to quantify the resilience margin of the wide-area damping control in a two-terminal VSC HVDC system against DoS and deception cyber-attacks. Furthermore, Fan et al. [111] assess the impacts of three cyber-attacks, i.e., timing attack, replay attack, and FDI attack, on a hybrid AC and two-terminal LCC HVDC system. In addition, Pan et al. [112] evaluate the impacts of DoS and FDI cyber-attacks on the load frequency control of a hybrid AC and two-terminal LCC HVDC system with emulated inertia.

4.2. During a cyber-attack event

For model-based cyber-attack detection, Chen et al. [23] propose a rule-based method to detect the FDI cyber-attacks on the wide-area damping control of a two-terminal LCC HVDC system. Moreover, Nuqui et al. [113] present an estimation-based detection method against FDI cyber-attacks on power order commands of a two-terminal LCC HVDC system. In addition, model-based detection methods against FDI cyber-attack on measurement data are proposed for a multi-terminal VSC HVDC system [114] and a series multi-terminal LCC HVDC system [115], respectively.

For data-driven cyber-attack detection, Sun et al. [116] propose a squeeze-excitation double conventional neural network to realize fast detection of the FDI cyber-attacks on phasor measurement unit data for the ancillary services of a two-terminal MMC HVDC system. Moreover, Roy et al. [117] present a multi-agent-based approach to detect cyber-attacks on the power modulation controller of a two-terminal VSC HVDC system. In addition, Chen et al. [118] propose a feedforward neural network-based method to detect the FDI cyber-attacks on measurement data of a two-terminal LCC

HVDC system.

4.3. After a cyber-attack event

First, for the VSC HVDC systems, Qiu et al. [119] propose a hybrid data-driven based ancillary control strategy to suppress the impacts of the FDI cyber-attacks on the phasor measurement unit data of a two-terminal VSC HVDC system. Moreover, Yao et al. [120] present a resilient wide-area damping control for a two-terminal VSC HVDC system against inter-area oscillations caused by deception cyber-attacks. Furthermore, Zhao et al. [121] propose a resilient adaptive wide-area damping control framework for a two-terminal VSC HVDC system against FDI cyber-attacks.

Second, for the MMC HVDC systems, Sun et al. [122] propose an attack-defense response control framework to mitigate the impacts of cyber-attacks on the communication of the wide-area measurement system in a two-terminal MMC HVDC system. In addition, [116] presents a frequency injection-based HVDC attack-defense control to suppress the potential impacts of FDI cyber-attacks on the MMC HVDC ancillary services. Third, for the LCC HVDC systems, based on a two-timescale cyber-attack evaluation model, Hou et al. [123] propose an event-triggered cybersecurity enhancement strategy against non-simultaneous cyber-attacks on a multi-infeed LCC HVDC system.

Remark: Although the two-terminal LCC HVDC system and the multi-terminal VSC HVDC system operate in different control strategies with different switching devices, both of them are intrinsically cyber-physical systems that suffer from malicious cyber-attacks on the inherent power electronics controllers. This could be dangerous for the power balances and secure operations of multiple asynchronously interconnected AC systems, which may result in unaffordable economic and social impacts.

5. Cyber resilience of prosumers

To curb carbon emissions and deal with climate change, the penetration level of renewable energy has increased dramatically. Hence, more and more power electronics devices are deployed in the power system since they are critical components in converting renewable energy into electricity. As a result, the proliferation of renewable energy has also transferred the role of traditional passive consumers into active prosumers, who are capable of producing power energy and interacting with the power grid. Therefore, more advanced communication infrastructures are needed for better demand-side management. However, more flexible interaction between users and the power grid also leads to more cyber vulnerability in communication security or physical device security. Identifying potential cyber threats and developing corresponding defense strategies are critical to enhancing the cyber resilience of prosumers. This review investigates the cyber resilience of three widely applied prosumers, i.e., the electric vehicle, the smart building, and the microgrid.

5.1. Electric vehicles

Driven by the low-carbon vision and sustainable policy, the penetration rate of electric vehicles is increasing significantly. According to the International Energy Agency [124], the number of electric vehicles on the road tripled within three years by 2021. The sales of electric vehicles nearly doubled in 2021 than 2020. The market share of electric vehicle sales in 2021 is about four times that of 2019. It is estimated that plug-in vehicle sales will reach 20.6 million in 2025, which is more than three times that of 2021 [125].

As electric vehicles have already become a significant part of both the power and transportation industry, concerns about cybersecurity issues are raised more frequently since manipulating the vehicles has been proven to be feasible [126]. In 2015, a Jeep Cherokee was remotely controlled and its acceleration and brakes are disabled [24]. Moreover, Tencent Keen Security Lab also proved the feasibility of remotely controlling the steering system and disturbing the autowipers function of Tesla [25]. In addition, Schneider Electric managed to identify cyber vulnerabilities of an electric vehicle charging station, get access full privileges, and influence the normal operation of devices [127].

In this regard, several cybersecurity standards are developed to ensure the safety of electric vehicles, including ISO/SAE 2143 [17], SAE J2847/1 [128], etc. In addition, several research projects are proposed to identify vulnerabilities and construct cyber-resilient electric vehicles, including Pacific Northwest National Laboratory [128], Sandia National Laboratory [41], National Renewable Energy Laboratory [126], and Idaho National Laboratory [129].

Among various cyber-attacks, the main cyber concerns for electric vehicles are the DoS cyber-attack, FDI cyber-attack, replay cyber-attack, and malware infection [130, 43]. Specifically, the potential cyber threats for electric vehicles include but are not limited to: 1) the communication links between electronic control units and subsystems inside electric vehicles [131]; 2) the frequent connection between the electric vehicle supply equipment and the electric vehicle in either a physical or wireless way [42]; 3) the multi-interface structure that provides more access points for malicious attacks [132]. This leads to the critical importance to address the cyber resilience of electric vehicles before, during, and after cyber-attack events.

5.1.1. Before a cyber-attack event

For cyber-attack impacts on local controllers of electric vehicles, Li et al. [133] adopt blockchain and fog computing technology to construct a charging scheme that is resilient to eavesdropping attacks and thus guarantees privacy. Dey et al. [134] propose a hardware-based real-time data processing algorithm for early detection and prevention of cyber-attacks that target the onboard charging system of electric vehicles. Wang et al. [135] establish an authentication protocol for electric vehicle charging using the Canetti and Krawczyk as the threat model, which can prevent potential cyber-attacks such as replay attacks and impersonation attacks. In addition, for cyber-attack impacts on grid-support functions of electric vehicles, Acharya et al. [136] design a demand-side data-driven cyber-attack strategy that can use plug-in electric vehicles to jeopardize the secure operation of a power system.

5.1.2. During a cyber-attack event

For the model-based cyber-attack detection method, Guo and Ye [137] propose an index-based evaluation metric and a coordinated detection method for electric vehicles with four motor drive systems. Dey and Khanra [138] propose a detection algorithm concerning the FDI attacks in battery packs of electric vehicles. Girdhar et al. [139] establish a Hidden-Markov-Model-based defense model considering the cybersecurity of an extremely fast charging station. The established defense model can detect malicious cyber intrusions, predict potential targets and generate defense strategies to mitigate attacks in multi-step scenarios. Abdollahi et al. [140] propose an observer-based control-oriented framework to deal with DoS attacks in connected vehicles. The proposed scheme can achieve real-time modeling and detection of DoS attacks as well as estimate the possible impact. In addition, for the data-driven cyber-attack method, Kavousi-Fard et al. [141] develop an anomaly detection model based on the generative adversarial network and the modified firefly algorithm to mitigate the vulnerability in the communication process between the electric control unit and other hardware units in the electric vehicle.

5.1.3. After a cyber-attack event

Rana [142] proposes an optimal state estimation and control algorithm against cyber-attacks in the communication channel of electric vehicles. Mousavian et al. [143] propose a response model to prevent the spread of malware in the electric vehicle supply equipment network. The model is formulated as a mixed integer linear programming problem that can jointly optimize the propagation risks and the disconnection level. Kabir et al. [144] establish a back propagation neural network-based detection scheme and an optimization-based wide-area controller against switching attacks in the charging network of electric vehicles.

5.2. Smart buildings

Buildings account for 36% of global energy demand and 37% of energy-related carbon emissions in 2020 [145]. A smart building, which is referred to as a building equipped with integrated technology systems [146], has attracted much attention due to its great potential for cutting down green house gas emissions. Typically, smart buildings contain multiple components, including the heating, ventilation, and air-conditioning (HVAC) system, lighting control system, metering, fire protection system, access control system, video surveillance system, vertical transport and facilities management system [147], etc. Those components jointly contribute to operational efficiency and service availability. In addition, the efficient energy usage and high-performance information communication capability enable a smart building with more flexibility to engage in demand-side management of power grids, leading to a grid-interactive building [148].

However, the interconnectivity and interoperability between subsystems as well as increasing digitization provide cyber-attack interfaces that exacerbate the building's confidentiality and security [147]. Multiple interfaces either in hardware or software may all become possible intrusion entrances. Attackers can get access to the control system to gain privilege, which makes it possible to directly control the physical equipment or steal private data [149]. More importantly, since a smart building usually interconnects with many outer devices and systems (e.g., electric vehicles, mobile phones, and power grids), it could become a medium to spread malicious attacks.

There are already reports about cyber-attacks on buildings. In Australia, it is demonstrated that the building management system of Google Australia Office can be hacked [26]. Target Corporation, one of the top retailers in the U.S., was hacked via HVAC systems using stolen network credentials, leading to approximately 40 million debit and credit card accounts exposition [27]. In the first half of 2019, it is estimated that nearly 40% smart building automation systems in 40,000 randomly selected samples have experienced malicious cyber-attacks [150]. This leads to the emerging need for cybersecurity standards of smart buildings, e.g., BACnet Secure Connect [18].

5.2.1. Before a cyber-attack event

Before cyber-attacks on a smart building, it is necessary to construct attack models, identify cyber vulnerabilities and potential attack paths. For instance, Fu et al. [151] propose a threat injection framework targeting energy simulators in buildings. The proposed framework is shown to be practical for energy simulators based on functional mock-up units. Moreover, Meyer et al. [152] propose a threat model and an attack tree for threat identification in building automation, which can help develop a more secure system.

5.2.2. During a cyber-attack event

During cyber-attacks on a smart building, timely detection and evaluation are necessary to stop the early spread of attacks and thus avoid negative impacts and subsequent cascading failures. For example, Sheikh et al. [153] develop a Boolean identification strategy to differentiate system faults or cyber-attacks in the HVAC system. Therein, the type of attacks are identified using the process control chart and day-ahead predicted logic. Furthermore, Fu et al. [154] establish a simulation-based modeling and evaluation framework for grid-interactive efficient buildings, which can quantify the impact of cyber-attacks on building operation services.

5.2.3. After a cyber-attack event

After cyber-attacks on a smart building, is it essential to construct resilient control strategies to maintain stable operation or recover from abnormal conditions as soon as possible. For instance, Paridari et al. [155] establish a cybersecurity framework for the building energy management system, which utilizes physical correlations between operating data for attack detection and resilient control. In addition, Xu et al. [156] construct a deep-learning-based HVAC control framework to enhance the fault tolerance ability when temperature sensors are experiencing passive faults or active cyber-attacks.

5.3. Microgrids

The microgrids with the integration of distributed energy resources are able to not only actively engage in demand-side management but also operate independently during power outages in the main power grid. As such, the microgrids manage to enhance power reliability, improve energy efficiency as well as facilitate the penetration of renewable energy sources [157]. Equipped with advanced information and automation infrastructure, a microgrid is intrinsically a cyber-physical system. Equipped with multiple power electronics-controlled devices, the microgrids are vulnerable to adversarial cyber-attacks [45] whether operated in isolated mode or in grid-connected mode, leading to catastrophic results on critical loads and interconnected grids [158].

Specifically, with threat modeling on microgrids [159, 160], the cyber threats of microgrids are: 1) multiple electronic-based devices as access points [158]; 2) internet exposure and communication inside and outside the microgrids [161]; 3) mismatch between legacy and new architectures [46]. To ensure the safety of microgrids, several standards and guidance are proposed, including: 1) IEEE 2030.9-2019 [162], i.e., IEEE recommended practice for the planning and design of the microgrid; 2) and a reference architecture proposed by Sandia National Laboratory [19]. Detailed studies regarding the cyber resilience of microgrids are investigated as follows.

5.3.1. Before a cyber-attack event

For cyber-attack impacts on local controllers, Zhang et al. [163] construct a concurrent attack model aiming at misleading local estimated and communicated voltages simultaneously in DC microgrids. Then, a detection strategy based on ensemble empirical mode decomposition is developed to avoid model-based detection and a criterion is proposed for attack classification. Nikmehr and Moradi [164] propose an attack model considering the FDI cyber-attack in microgrid control centers. The game-theory approach is then adopted to model the attack-and-defend interaction between microgrids. In addition, for cyber-attack impacts on grid-support functions, Mohamed et al. [165] prove that the FDI cyber-attack is able to influence the synchronization of microgrids. An analytical framework is presented to provide success conditions for the attacks as well as the weakness of the synchronization system. Then, two mitigation strategy is devised to prevent potential attacks.

5.3.2. During a cyber-attack event

To prevent cyber-attacks from jeopardizing the secure operation of microgrids and interconnected systems, efficient detection and defense strategies are necessary. For instance, Saad et al. [166] introduce the Internet of Thing-based digital twin to develop a framework that can detect and respond to cyber-attacks in networked microgrids. In addition, Hao et al. [167] develop an adaptive Markov defending strategy to estimate the attacker's behavior and make adaptive responses in order to prevent jeopardizing the secure operation of microgrids.

5.3.3. After a cyber-attack event

In [168], a resilient controller based on a two-layer augmented linear quadratic regulator and unknown input observer is proposed. The proposed controller can achieve frequency control of microgrids under FDI cyber-attacks and enhance the resilience of microgrids. Moreover, Khalghani et al. [169] propose a hidden layer-based distributed cooperative control algorithm to maintain the stability of the islanded microgrids under FDI cyber-attacks. Furthermore, Liu et al. [170] propose an optimal frequency control scheme for distributively controlled microgrids. The proposed robust algorithm can withstand cyber-attacks within certain ranges or isolate the contaminated information from spreading when attacks are out of bounds. In addition, Chlela et al. [171] propose a fullback control strategy to defend DoS cyber-attacks, which can be used in 100% inverter-interfaced microgrids.

Remark: The power electronics devices in power prosumption (e.g., electric vehicles, smart buildings, microgrids) are closely related to the end-users. In other words, the cyber-attack surface is geographically widespread and the cyber-attack-induced consequences would have direct impacts on people. In this regard, the cyber-attacks on a power electronics device in power prosumption may result in safety hazards to: 1) other power electronics devices (e.g., vehicle to vehicle [132]); 2) human beings (e.g., vehicle to pedestrian [131]); 3) the whole power grid (e.g., vehicle to grid [172], grid-interactive buildings [148]); 4) the smart city [173, 149]. To this end, the immature communication protocols [131] and unregulated cybersecurity standards [174] of power electronics devices in power prosumption should be further improved.

6. Cyber resilience of energy storage systems

Since power systems are integrated with increasing penetration of renewable energy resources, the energy storage systems become a key component against the intermittency and volatility either in generations or loads [175]. In addition, the prosperity of electric vehicles also contributes to the expansion of energy storage. As a result, the size of stationary and transportation energy storage combined markets will be three to five times the current level by 2030 [176].

Typically, an energy storage system interconnected to a power grid consists of the battery pack, power conversion system, battery management systems, supervisory control system, and communication system [48]. As a cyber-physical system, the energy storage system is also prone to various cyber-attacks. For example, it is demonstrated that the smart battery controller of MacBook can be hacked and the battery data can be maliciously modified, leading to safety hazards, such as overcharging or fire [29]. More importantly, since the energy storage systems are usually embedded in electric vehicles, smart buildings, and power grids, the cyber-attacks on an energy storage system could be propagated to other devices, leading to possible cascading failures.

Therefore, several cybersecurity-related roadmaps and standards are proposed, including: 1) the critical infrastructure protection standard proposed by North American Electric Reliability Corporation [177]; 2) IEEE standard 2030.2-2015, i.e., IEEE Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure [178]; 3) Standard for the Installation of Stationary Energy Storage Systems proposed by National

Fire Protection Association [179]; 4) Energy Storage Systems Safety Roadmap proposed by U.S. Department of Energy [180].

6.1. Before a cyber-attack event

Zhuang and Liang [181] investigate the theoretical principle of constructing the FDI cyber-attacks targeting at state-of-charge estimation inside an energy storage system. Then, sequential FDI cyber-attacks and an online construction method are proposed. In addition, using artificial neural networks, Pasetti et al. [182] demonstrate the feasibility of man-in-the-middle attacks against energy storage systems.

6.2. During a cyber-attack event

Lee et al. [183] establish a fault diagnosis model based on convolutional neural networks to evaluate the trustworthiness of battery data in energy storage systems. The proposed model can detect and classify battery faults caused by different reasons, such as sensor faults, communication failures, and cyber-attacks. Farraj et al. [184] address the impact of FDI cyber-attacks on storage-based transient stability control. Closed-form expressions of rotor dynamics are derived considering FDI cyber-attacks on the parametric feedback linearization control.

6.3. After a cyber-attack event

Ding et al. [185] propose an acknowledgment-based detection strategy and a communication recovery mechanism to defend the DoS attacks targeting heterogeneous energy storage systems. Then, a distributed secondary control scheme is proposed to maintain the secure operation of energy storage systems with finite time. Moreover, Chen et al. [186] propose a decentralized secondary control scheme for multiple heterogeneous battery energy storage systems against DoS cyber-attacks. Therein, a strategy based on signal-to-interference-plus-noise-ratio is constructed to ease the burden of communication resources occupation under DoS attacks. Furthermore, Deng et al. [187] develop a distributed resilient control strategy based on an adaptive technique for multiple energy storage systems in islanded microgrids. Therein, the stability of the systems under unknown faults and cyber-attacks can be guaranteed using the Lyapunov method. In addition, Sharma et al. [188] establish a fuzzy logic-based cyber-attack detection scheme for distributed energy storage systems. Therein, a consensus-based leader-follower distributed control strategy is proposed to ensure stable operation under cyber-attacks.

7. Discussion regarding the cybersecurity paradigm shift from power grids to power electronics devices

7.1. General cyber threats of power electronics devices

For comparison, the cyber resilience of each power electronics device is illustrated in Table 4. Since the power electronics-enabled power system consists of multiple cyber-physical subsystems in each power electronics device, previous studies have made significant efforts to enhance cyber resilience against potential cyber threats. Therein, two general cyber threats of power electronics devices are summarized as follows.

One general cyber threat of the power electronics devices inside a power system is the closed-loop feedback controllers that rely on real-time measurement data. To detect and distinguish the natural noises and/or malicious injections in measurement data, the power system control center implements bad data detection (e.g., the largest normalized residual test [189]) before delivering the verified measurement to the subsequent applications. However, nearly no power electronics controllers have similar default detection mechanisms before adopting the measurement data as control inputs. This is a critical cyber vulnerability since the measurement data that are either locally collected or remotely transmitted could be possibly compromised by many kinds of cyber-attacks. As a result, the compromised power electronics controllers (e.g., voltage controller, current controller, power controller, etc.) may cause severe damage to the power electronics devices, including overvoltage [59], overcurrent, etc. More importantly, since the interconnected power electronics devices usually have multiple grid-support functions, the compromised power electronics controllers could also jeopardize the secure operation of power grids, leading to active power imbalances [123], frequency and voltage deviations [190], and subsequent affordable consequences.

The other general cyber threat of the power electronics devices inside a power system is the substantial number of communication infrastructures among geographically widespread devices. The cyber threat is driven by multiple motivations, including but not limited to [14, 191]: 1) the trend towards collective and/or coordination control strategy; 2) the need for distant control and communication due to remotely located devices; 3) additional access points from both hardware modifications and software injections; 4) publicly accessible internet due to multi-stakeholder environment and varying device stewardship.

Table 4: Representative cyber resilience enhancement strategies of power electronics devices before, during, and after cyber-attack events

	Power electronics devices	Identification strategies before cyber events	Detection strategies during cyber events	Responsive strategies after cyber events
Converter	VSC	[50, 57, 58]	[59, 60, 61]	[62, 63, 64]
Generation	wind	[85, 89, 90]	[92, 93]	[94, 95]
	photovoltaic	[70, 71]	[67, 72, 74]	-
Transmission	HVDC	[109, 110, 112]	[23, 116, 117]	[120, 122, 123]
Prosumption	electric vehicle	[133, 135, 136]	[137, 138, 139]	[142, 143, 144]
	smart building	[151, 152]	[153, 154]	[155, 156]
	microgrid	[163, 164, 165]	[166, 167]	[168, 169, 170]
Storage		[181, 182]	[183, 184]	[185, 186, 187]

7.2. Cybersecurity paradigm shift from power grids to power electronics devices

For comparison, the similarities and differences of cybersecurity paradigms between power electronics devices and power grids are illustrated in Table 5. The similarities are manifested in two folds. First, both the power electronics device and the power grid suffer from cyber-attacks on measurement data and command data. This is achieved by manipulating the metering and communication infrastructures using data integrity attacks (e.g., the FDI attack), data availability attacks (e.g., the DoS attack), and data confidentiality attacks (e.g., malware). Second, the cyber resilience of both the power electronics

Table 5: Similarities and differences of the cyber resilience between power electronics devices and power grids

		power grid	**power electronics**
		OPF control	**general control**
difference	**paradigm**	open-loop control (measurement is independent of control output)	closed-loop controller (measurement is feedback of control output)
	timescale	long (minutes/hours)	short (milliseconds/seconds)
	stealthiness	achieved by satisfying power flow equation	achieved by corrective action of closed-loop controller
	communication	centralized architecture	decentralized/distributed architecture
similarity	cyber-attack	data integrity/availability/confidentiality cyber-attack on measurement/command data via metering/communication infrastructures	
	cyber-defense	identification/detection/response cyber-defense strategies before/during/after cyber-attacks	

device and the power grid could be enhanced in three stages, i.e., before, during, and after cyber-attack events. This is achieved by 1) identifying cyber vulnerabilities of the system model; 2) detecting cyber-attack injections on measurement/command data; 3) respond and mitigate the cyber-attack-induced consequences. Note that the cyber-defense strategies in three stages could be implemented in either an independent or coordinated manner.

The differences of cybersecurity paradigms between power electronics devices and power grids are manifested in several folds. First, as shown in Fig. 10, one significant cybersecurity paradigm shift from power grids to power electronics devices is the transition from an open-loop paradigm to a closed-loop paradigm. The closed-loop cybersecurity paradigm indicates that the measurement of the power electronics controllers is the feedback of control outputs, while the open-loop cybersecurity paradigm indicates that the measurement of the power grid applications is independent of control outputs.

For instance, the cyber-attacks on a power grid application (e.g., the

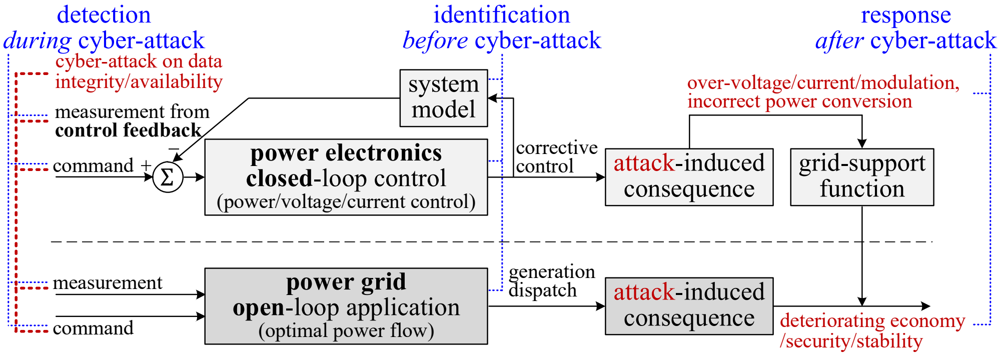


Figure 10: Comparison of the cyber attack/defense paradigms between the power electronics closed-loop control and the power grid open-loop application.

widely applied optimal power flow (OPF)) are designed to compromise the measurement data (e.g., the real-time loads) that are independent of the decision-making (e.g., the generation outputs). This could result in inappropriate re-dispatch of generations, leading to the deterioration of power system economy [192], security [193], stability [194], etc. By comparison, the power electronics controllers i.e., closed-loop feedback controllers, are designed to accurately and rapidly regulate the measurement feedback so as to track the varying command. In other words, once the measurement and/or command data are compromised, the corrective actions of the closed-loop power electronics controllers (e.g., voltage/current/power controllers) would lead to overvoltage, overcurrent, etc. This could jeopardize not only the power electronics device but also the interconnected power grid.

Second, the timescales of the cyber-attack-induced consequences are different. For the power grid OPF control, the cyber-attack-induced re-dispatch of OPF [192] is usually in the time span of minutes [189]. By comparison, the cyber-attack-induced overvoltage of a converter voltage controller [59] is usually in the time span of milliseconds. This implies that the cyber defenders for a power electronics device have little time to detect, locate, and mitigate the cyber-attacks before irreversible consequences.

Third, the cyber-attack stealthiness on power grids and power electronics devices are achieved in an active manner and reactive manner, respectively. From the viewpoint of the power system OPF, the FDI cyber-attack is stealthy if the cyber-attack injections satisfy the power flow equation [195] and thus bypass the bad data detection. By comparison, it is interesting to find that FDI cyber-attacks on measurement data are also stealthy to power electronics controllers [59]. This is due to the corrective action of the closed-loop power electronics controller, which consistently eliminates the difference between the command and the possibly compromised measurement.

Fourth, the main cyber threats are manifested in different communication architectures. Typically, a power grid is operated by the control center with a centralized control and communication architecture. That is, data are transmitted between the control center and other globally widespread devices. It is the cyber-attack on the centralized communication architecture that threatens the power grid secure operation. By comparison, a power electronics device is controlled in a decentralized communication architecture (via locally collected measurement [23]) or distributed communication architecture (via information sharing with surrounding devices [59]). It is the cyber-attack on the decentralized or distributed communication architecture that threatens the secure operation of the power electronics device.

7.3. Limitations

The major limitations of this review are discussed to provide insights for future directions. First, although the cyber resilience enhancement strategies before, during, and after cyber-attack events are investigated, the operational costs and control efforts to achieve the cyber-defense strategies are not clearly addressed. In other words, the cyber-defense strategies on power electronics devices may require additional economic investments and/or deteriorate controllers' performance. Therefore, it is needed in future work to consider not only the effectiveness but also the cost-effectiveness when addressing a cyber resilience enhancement strategy before, during, and after cyber-attack events. This is practical for not only power system operators but also stakeholders of the integrated power electronics devices.

Second, this review only investigates the cyber resilience enhancement strategies from the viewpoint of a cyber defender, which may not be sufficient to counteract state-of-the-art cyber-attacks. For instance, the choice of the most damaging attacking purpose from a cyber attacker may be different from the one from a cyber defender. In this regard, the viewpoints from both a cyber defender and a cyber attacker are needed to comprehensively address the cyber resilience of power electronics-enabled power systems.

8. Conclusions and future trends

8.1. Conclusions

Empowering energy infrastructures with physical resilience has been well investigated, but it has not been well addressed to construct a cyber-resilient energy infrastructure that equips the capability to anticipate, absorb, adapt to, and rapidly recover from a potentially disruptive cyber-attack event. In particular, since the current power systems are integrated with increasing power electronics devices and related access points, the potentially destructive cyber-attacks could result in severe consequences with increasingly high probability, which are rarely considered in the traditional methodology. To this end, this review comprehensively investigates the cyber resilience of power electronics-enabled power systems from three aspects, i.e., before, during, and after cyber-attack events. Therein, the representative cyber-attack events, cyber-defense threats, and cybersecurity regulations of multiple power electronics devices (in power generation, power transmission, power prosumption, and power storage) are addressed, respectively. More importantly, this review proposes a general cybersecurity paradigm of power electronics closed-loop controllers, which is different from the one of power grid open-loop applications.

The stakeholders of all the integrated power electronics devices could benefit from this review in terms of constructing a cyber-resilient framework before, during, and after potential cyber-attacks. Then, the power grid operators can make use of this review to implement effective and cost-effective cyber-defense strategies. In the long term, this review facilitates policy-makers to propose power electronics-oriented cybersecurity standards and regulations, which help establish social, economic, and environmental resilience.

8.2. Future directions

The trend toward a power electronics-intensive power system has been accelerating due to the urgent demand for carbon neutrality. Nevertheless, the cyber resilience solutions catering specifically to the power electronics-enabled power system are still in the early days of development. Hence, there remain lots of unsolved problems and undiscovered future directions from the viewpoints of either a cyber defender or a cyber attacker.

From the viewpoint of a cyber defender, one promising future direction for the cyber resilience of the power electronics-enabled power system is the trade-off between cybersecurity and controllability. For instance, there exists a conflict between the control performance and the intrusion detection rate due to the following reasons. First, the power electronics controller should quickly regulate the small fluctuations between the command and the real-time measurement. Second, it should also rapidly suppress large disturbances to avoid severe faults. Third, the power electronics controllers are usually controlled in the time span of milliseconds or seconds and thus have little time for detection. To this end, it is necessary to investigate how to concurrently ensure cyber resilience and guarantee controllability.

To provide insight for system operators, one future direction from the viewpoint of a cyber attacker is the cost-effectiveness of the cyber-attacks on the power electronics-enabled power system. The cyber-attacks on a traditional SG-based power system have been demonstrated to achieve different attacking purposes, including the economy (e.g., maximum of operation costs [192], illegal profits from electricity markets [196]), security (e.g., line overloading [193]), stability (e.g., deterioration of stability margin [194]), etc. To this end, how to achieve different and multiple attack purposes on a power electronics-enabled power system and how to achieve the cost-benefit trade-off of implementing such cyber-attacks would be promising research directions.

Appendix A. Cybersecurity regulations and roadmaps for power systems and power electronics devices

Table A.1: Cybersecurity regulations and roadmaps for power systems

Category	Regulation and Roadmap	Institution	Time	Ref
cybersecurity of critical infrastructure	NIST critical infrastructure protection (NIST: National Institute of Standards and Technology)	NIST	2018	[177]
	cyber intrusion guide for system operators (NERC: North American Electric Reliability Corporation)	NERC	2018	[197]
cybersecurity of industrial control system	IEC 62443 for industrial communication networks (IEC: International Electrotechnical Commission)	IEC	2007	[10]
	ISO/IEC 27000 for information security (ISO: International Organization for Standardization)	ISO	2018	[198]
cybersecurity of power system	IEC 62351 for data and communications security	IEC	2007	[9]
	NIST 7628 for for smart grid cybersecurity	NIST	2010	[11]
	IEEE C37.240 for substation automation	IEEE	2015	[199]
cybersecurity of power electronics devices	IEEE 1686-2007 for intelligent electronic devices	IEEE	2007	[12]
	IEEE 1547-2018 for distributed energy resources	IEEE	2018	[15]
	NIST technical note 2182 for distributed energy resources	NIST	2021	[191]

Table A.2: Cybersecurity regulations and roadmaps for representative power electronics devices in power systems

Category	Device	Regulation (Institution)	Time	Ref
Generation Cybersecurity	photovoltaic	roadmap for photovoltaic cyber security (Sandia National Laboratory)	2017	[13]
		cybersecurity in photovoltaic plant operations (National Renewable Energy Laboratory)	2021	[22]
	wind	roadmap for wind cybersecurity (U.S. Department of Energy)	2020	[14]
		cybersecurity guide for distributed wind (U.S. Department of Energy)	2019	[37]
		IEC 61400-25-1 for wind power plants (IEC: International Electrotechnical Commission)	2017	[200]
Transmission Cybersecurity	HVDC	cyber-attack resilient HVDC (U.S. Department of Energy)	2019	[16]
		cyber security services of HVDC (Hitachi Energy)	2020	[107]
Prosumption Cybersecurity	electric vehicle	SAE J2847/1 for electric vehicle communication (SAE: Society of Automotive Engineers)	2014	[128]
		ISO/SAE 2143 for automotive cybersecurity (ISO: International Organization for Standardization)	2021	[17]
	microgrid	IEEE 2030.9-2019 for microgrid design (IEEE)	2019	[162]
		microgrid cybersecurity reference architecture (Sandia National Laboratory)	2015	[19]
	smart building	BACnet secure connect (BACnet: Building Automation and Control networks)	2020	[18]
Storage Cybersecurity	energy storage	IEEE 2030.2-2015 for energy storage system (IEEE)	2015	[178]
		NFPA 855 for stationary energy storage system (NFPA: National Fire Protection Association)	2019	[180]

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 52177118, and in part by the Collaborative Research Fund (CRF Project No. C1052-21GF) from the Research Grants Council, Hong Kong SAR. The work of Shunbo Lei was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 52307145, and in part by the Shenzhen Key Laboratory of Crowd Intelligence Empowered Low-Carbon Energy Network (ZDSYS20220606100601002).

Declaration of competing interest

The authors declare the following personal relationships which may be considered as potential competing interests: Dr. Yunhe Hou on this paper is a guest editor, he was blinded during the review process and this review was handled by another editor.

References

[1] Net zero by 2050 - a roadmap for the global energy sector, Technical report, International Energy Agency (2021).
URL `https://iea.blob.core.windows.net/assets/deebef5d-0c34-4539-9d0c-10b13d840027/NetZeroby2050-ARoadmapfortheGlobalEnergySector_CORR.pdf`

[2] B. Kroposki, B. Johnson, Y. Zhang, V. Gevorgian, P. Denholm, B.-M. Hodge, B. Hannegan, Achieving a 100% renewable grid: Operating electric power systems with extremely high levels of variable renewable

energy, IEEE Power and Energy Magazine 15 (2) (2017) 61–73. doi:10.1109/MPE.2016.2637122.

[3] Q.-C. Zhong, Power-electronics-enabled autonomous power systems: Architecture and technical routes, IEEE Transactions on Industrial Electronics 64 (7) (2017) 5907–5918. doi:10.1109/TIE.2017.2677339.

[4] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli, Cyber–physical security of a smart grid infrastructure, Proceedings of the IEEE 100 (1) (2012) 195–209. doi:10.1109/JPROC.2011.2161428.

[5] J. C. Balda, A. Mantooth, R. Blum, P. Tenti, Cybersecurity and power electronics: Addressing the security vulnerabilities of the internet of things, IEEE Power Electronics Magazine 4 (4) (2017) 37–43. doi:10.1109/MPEL.2017.2761422.

[6] S. K. Mazumder, A. Kulkarni, S. Sahoo, F. Blaabjerg, H. A. Mantooth, J. C. Balda, Y. Zhao, J. A. Ramos-Ruiz, P. N. Enjeti, P. R. Kumar, L. Xie, J. H. Enslin, B. Ozpineci, A. Annaswamy, H. L. Ginn, F. Qiu, J. Liu, B. Smida, C. Ogilvie, J. Ospina, C. Konstantinou, M. Stanovich, K. Schoder, M. Steurer, T. Vu, L. He, E. P. de la Fuente, A review of current research trends in power-electronic innovations in cyber–physical systems, IEEE Journal of Emerging and Selected Topics in Power Electronics 9 (5) (2021) 5146–5163. doi:10.1109/JESTPE.2021.3051876.

[7] Enhancing cyber resilience in electricity systems, Technical report, International Energy Agency (2021).

URL https://iea.blob.core.windows.net/assets/0ddf8935-be23-4d5f-b798-3aad1f32432f/Enhancing_Cyber_Resilience_in_Electricity_Systems.pdf

[8] A. Khan, M. Hosseinzadehtaher, M. B. Shadmand, S. Bayhan, H. Abu-Rub, On the stability of the power electronics-dominated grid: A new energy paradigm, IEEE Industrial Electronics Magazine 14 (4) (2020) 65–78. doi:10.1109/MIE.2020.3002523.

[9] Power systems management and associated information exchange, data and communications security (IEC 62351), Tech. rep., International Electrotechnical Commission Standard (IEC) (2007).

[10] Industrial communication networks and system security part 1-1: Terminology, concepts and models. (IEC 62443), Tech. rep., International Electrotechnical Commission (IEC) (2009).

[11] Guidelines for smart grid cybersecurity. (NIST interagency report 7628), Tech. rep., National Institute of Standards and Technology (NIST) (2010).

[12] IEEE standard for intelligent electronic devices cyber security capabilities (2014) 1–29 doi:10.1109/IEEESTD.2014.6704702.

[13] Roadmap for PV cyber security, Tech. rep., Sandia National Lab (2017). doi:10.2172/1782667.
URL https://www.osti.gov/biblio/1782667

[14] Roadmap for wind cybersecurity, Tech. rep., Idaho National Lab (2020).

doi:10.2172/1647705.
URL https://www.osti.gov/biblio/1647705

[15] IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces (2018) 1–138 doi:10.1109/IEEESTD.2018.IEEEStd_1547_DER_2018.

[16] R. Nuqui, Cyber attack resilient HVDC system (CARDS) (final scientific/technical report), Tech. rep., ABB Inc. (2019). doi:10.2172/1810571.
URL https://www.osti.gov/biblio/1810571

[17] Automotive cybersecurity: An introduction to ISO/SAE 21434, Tech. rep., ISO (International Organization for Standardization) and SAE (Society of Automotive Engineers) (2021).

[18] BACnet secure connect: The next generation of OT security for building operations, Tech. rep., Siemens (2020).
URL https://assets.new.siemens.com/siemens/assets/api/uuid:a450472e-bfbf-4fff-b8a1-b98a22bce1b7/cybersecurity-for-building-operations-white-paper-by-siemens.pdf

[19] J. E. Stamp, C. K. Veitch, J. M. Henry, D. H. Hart, B. Richardson, Microgrid cyber security reference architecture (v2)., Tech. rep., Sandia National Lab (2015).

[20] R. D. Trevizan, Cybersecurity of battery energy storage systems., Tech. rep., Sandia National Lab (2021).
URL https://www.osti.gov/servlets/purl/1855330

[21] R. E. Mackiewicz, Overview of IEC 61850 and benefits, in: 2006 IEEE Power Engineering Society General Meeting, IEEE, 2006, pp. 8–pp.

[22] A. Walker, J. Desai, D. Saleem, T. Gunda, Cybersecurity in photovoltaic plant operations (3 2021). doi:10.2172/1774870.
URL https://www.osti.gov/biblio/1774870

[23] B. Chen, S.-i. Yim, H. Kim, A. Kondabathini, R. Nuqui, Cybersecurity of wide area monitoring, protection, and control systems for HVDC applications, IEEE Transactions on Power Systems 36 (1) (2021) 592–602. doi:10.1109/TPWRS.2020.3022588.

[24] C. Miller, C. Valasek, Remote exploitation of an unaltered passenger vehicle, Black Hat USA (2015).

[25] T. K. S. Lab, Experimental security research of Tesla autopilot (2019).

[26] K. Zetter, Researchers hack building control system at google australia office (2013).
URL https://www.wired.com/2013/05/googles-control-system-hacked/

[27] B. Krebs, Target hackers broke in via HVAC company, Krebs on Security 5 (2014).

[28] D. U. Case, Analysis of the cyber attack on the Ukrainian power grid, Electricity Information Sharing and Analysis Center (E-ISAC) 388 (2016) 1–29.

[29] C. Miller, Battery firmware hacking, Black Hat USA (2011) 3–4.

[30] Keeping the country running: natural hazards and infrastructure, Tech. rep., Cabinet Office (2011).

[31] L. Xu, Q. Guo, Y. Sheng, S. Muyeen, H. Sun, On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective, Renewable and Sustainable Energy Reviews 152 (2021) 111642. `doi:https://doi.org/10.1016/j.rser.2021.111642`.
URL `https://www.sciencedirect.com/science/article/pii/S1364032121009175`

[32] W. Xu, F. Teng, A deep learning based detection method for combined integrity-availability cyber attacks in power system (2020). `doi:10.48550/ARXIV.2011.01816`.
URL `https://arxiv.org/abs/2011.01816`

[33] S. Ahmadi, Y. Saboohi, A. Vakili, Frameworks, quantitative indicators, characters, and modeling approaches to analysis of energy system resilience: A review, Renewable and Sustainable Energy Reviews 144 (2021) 110988. `doi:https://doi.org/10.1016/j.rser.2021.110988`.
URL `https://www.sciencedirect.com/science/article/pii/S136403212100280X`

[34] A. Younesi, H. Shayeghi, Z. Wang, P. Siano, A. Mehrizi-Sani, A. Safari, Trends in modern power systems resilience: State-of-the-art review, Renewable and Sustainable Energy Reviews 162 (2022) 112397. `doi:https://doi.org/10.1016/j.rser.2022.112397`.

URL https://www.sciencedirect.com/science/article/pii/S1364032122003070

[35] J. Jasiūnas, P. D. Lund, J. Mikkola, Energy system resilience – a review, Renewable and Sustainable Energy Reviews 150 (2021) 111476. doi:https://doi.org/10.1016/j.rser.2021.111476.
URL https://www.sciencedirect.com/science/article/pii/S1364032121007577

[36] J. T. Johnson, PV cybersecurity final report. (1 2019). doi:10.2172/1491601.
URL https://www.osti.gov/biblio/1491601

[37] M. J. Culler, J. P. Gentle, B. Smith, F. Cleaveland, S. Morash, Cybersecurity guide for distributed wind (9 2021). doi:10.2172/1826578.
URL https://www.osti.gov/biblio/1826578

[38] J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, T. Kim, J. Liu, B. Chen, G.-S. Seo, W. Song, M. D. R. Greidanus, S. Sahoo, F. Blaabjerg, J. Zhang, L. Guo, B. Ahn, M. B. Shadmand, N. R. Gajanur, M. A. Abbaszada, A review of cyber–physical security for photovoltaic systems, IEEE Journal of Emerging and Selected Topics in Power Electronics 10 (4) (2022) 4879–4901. doi:10.1109/JESTPE.2021.3111728.

[39] I. Zografopoulos, C. Konstantinou, N. D. Hatziargyriou, Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts,

and mitigations (2022). doi:10.48550/ARXIV.2205.11171.
URL https://arxiv.org/abs/2205.11171

[40] N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, G. Fujita, A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy, IEEE Access 10 (2022) 35846–35875. doi:10.1109/ACCESS.2022.3163551.

[41] Securing vehicle charging infrastructure against cybersecurity threats, Tech. rep., Sandia National Laboratory (2020).
URL https://www.osti.gov/servlets/purl/1763166

[42] J. Johnson, T. Berg, B. Anderson, B. Wright, Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses, Energies 15 (11) (2022) 3931. doi:10.3390/en15113931.

[43] M. Dibaei, X. Zheng, K. Jiang, R. Abbas, S. Liu, Y. Zhang, Y. Xiang, S. Yu, Attacks and defences on intelligent connected vehicles: A survey, Digital Communications and Networks 6 (4) (2020) 399–421. doi:https://doi.org/10.1016/j.dcan.2020.04.007.

[44] G. Li, L. Ren, Y. Fu, Z. Yang, V. Adetola, J. Wen, Q. Zhu, T. Wu, K. Candan, Z. O'Neill, A critical review of cyber-physical security for building automation systems, Annual Reviews in Control (2023). doi:https://doi.org/10.1016/j.arcontrol.2023.02.004.
URL https://www.sciencedirect.com/science/article/pii/S1367578823000032

[45] G. B. Gaggero, P. Girdinio, M. Marchese, Advancements and research trends in microgrids cybersecurity, Applied Sciences 11 (16) (2021) 7363. doi:10.3390/app11167363.

[46] N. Jamil, Q. S. Qassim, F. A. Bohani, M. Mansor, V. K. Ramachandaramurthy, Cybersecurity of microgrid: State-of-the-art review and possible directions of future research, Applied Sciences 11 (21) (2021) 9812. doi:10.3390/app11219812.

[47] R. D. Trevizan, J. Obert, V. De Angelis, T. A. Nguyen, V. S. Rao, B. R. Chalamala, Cyberphysical security of grid battery energy storage systems, IEEE Access 10 (2022) 59675–59722. doi:10.1109/ACCESS.2022.3178987.

[48] J. Johnson, J. Hoaglund, R. Trevizan, T. Nguyen, Chapter 18: Physical Security and Cybersecurity of Energy Storage Systems, 2021. URL https://www.sandia.gov/app/uploads/sites/163/2021/09/ESHB_Ch18_Physical-Security_Johnson.pdf

[49] Y. Li, J. Yan, Cybersecurity of smart inverters in the smart grid: A survey, IEEE Transactions on Power Electronics 38 (2) (2023) 2364–2383. doi:10.1109/TPEL.2022.3206239.

[50] S. Sahoo, T. Dragičević, F. Blaabjerg, Cyber security in control of grid-tied power electronic converters—challenges and vulnerabilities, IEEE Journal of Emerging and Selected Topics in Power Electronics 9 (5) (2021) 5326–5340. doi:10.1109/JESTPE.2019.2953480.

[51] B. Mirafzal, A. Adib, On grid-interactive smart inverters: Features and advancements, IEEE Access 8 (2020) 160526–160536. doi:10.1109/ACCESS.2020.3020965.

[52] N. Pogaku, M. Prodanovic, T. C. Green, Modeling, analysis and testing of autonomous operation of an inverter-based microgrid, IEEE Transactions on Power Electronics 22 (2) (2007) 613–625. doi:10.1109/TPEL.2006.890003.

[53] A. Fernández-Guillamón, E. Gómez-Lázaro, E. Muljadi, Ángel Molina-García, Power systems with high renewable energy sources: A review of inertia and frequency control strategies over time, Renewable and Sustainable Energy Reviews 115 (2019) 109369. doi:https://doi.org/10.1016/j.rser.2019.109369.
URL https://www.sciencedirect.com/science/article/pii/S1364032119305775

[54] R. Cresap, W. Mittelstadt, Small-signal modulation of the pacific HVDC intertie, IEEE Transactions on Power Apparatus and Systems 95 (2) (1976) 536–541. doi:10.1109/T-PAS.1976.32133.

[55] Y. Liu, Y. Song, Z. Wang, C. Shen, Optimal emergency frequency control based on coordinated droop in multi-infeed hybrid ac-dc system, IEEE Transactions on Power Systems 36 (4) (2021) 3305–3316. doi:10.1109/TPWRS.2021.3052251.

[56] A. de la Villa Jaen, E. Acha, A. G. Exposito, Voltage source converter modeling for power system state estimation: STATCOM and VSC-

HVDC, IEEE Transactions on Power Systems 23 (4) (2008) 1552–1559. doi:10.1109/TPWRS.2008.2004821.

[57] I. Zografopoulos, J. Ospina, X. Liu, C. Konstantinou, Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies, IEEE Access 9 (2021) 29775–29818. doi:10.1109/ACCESS.2021.3058403.

[58] A. Barua, M. A. Al Faruque, Hall spoofing: a noninvasive dos attack on grid-tied solar inverter, in: Proceedings of the 29th USENIX Conference on Security Symposium, 2020, pp. 1273–1290.
URL https://www.usenix.org/system/files/sec20-barua.pdf

[59] C. Burgos-Mellado, F. Donoso, T. Dragičević, R. Cárdenas-Dobson, P. Wheeler, J. Clare, A. Watson, Cyber-attacks in modular multilevel converters, IEEE Transactions on Power Electronics 37 (7) (2022) 8488–8501. doi:10.1109/TPEL.2022.3147466.

[60] J. Zhang, J. Ye, Cyber-attack detection for active neutral point clamped (ANPC) photovoltaic (PV) converter using kalman filter, in: 2022 IEEE Applied Power Electronics Conference and Exposition (APEC), 2022, pp. 1939–1944. doi:10.1109/APEC43599.2022.9773382.

[61] F. Li, Q. Li, J. Zhang, J. Kou, J. Ye, W. Song, H. A. Mantooth, Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network, IEEE Transactions on Power Electronics 36 (3) (2021) 2495–2498. doi:10.1109/TPEL.2020.3017935.

[62] Y. Wang, S. Mondal, C. Deng, K. Satpathi, Y. Xu, S. Dasgupta, Cyber-resilient cooperative control of bidirectional interlinking converters in networked ac/dc microgrids, IEEE Transactions on Industrial Electronics 68 (10) (2021) 9707–9718. doi:10.1109/TIE.2020.3020033.

[63] S. Sahoo, T. Dragičević, Y. Yang, F. Blaabjerg, Adaptive resilient operation of cooperative grid-forming converters under cyber attacks, in: 2020 IEEE CyberPELS (CyberPELS), 2020, pp. 1–5. doi:10.1109/CyberPELS49534.2020.9311543.

[64] Y. Chen, W. Qiu, X. Liu, Y. Kang, A parallel control framework of analog proportional integral and digital model predictive controllers for enhancing power converters cybersecurity, IEEE Journal of Emerging and Selected Topics in Power Electronics 10 (1) (2022) 1258–1269. doi:10.1109/JESTPE.2019.2937800.

[65] Solar PV, Tech. rep., International Energy Agency (IEA) (2022).
URL https://www.iea.org/reports/solar-pv

[66] R. Margolis, Solar futures study databook, Tech. rep., National Renewable Energy Laboratory (2021).
URL https://www.osti.gov/biblio/1830416

[67] L. Guo, J. Zhang, J. Ye, S. J. Coshatt, W. Song, Data-driven cyber-attack detection for PV farms via time-frequency domain features, IEEE Transactions on Smart Grid 13 (2) (2022) 1582–1597. doi:10.1109/TSG.2021.3136559.

[68] C. Carter, C. Lai, N. Jacobs, S. Hossain-McKenzie, P. Cordeiro, I. Onunkwo, J. T. Johnson, Cyber security primer for DER vendors aggregators and grid operators (11 2017). doi:10.2172/1761987. URL https://www.osti.gov/biblio/1761987

[69] J. T. Johnson, Secure scalable control and communications for distributed PV (final technical report) (1 2019). doi:10.2172/1761981. URL https://www.osti.gov/biblio/1761981

[70] X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, X. Liu, Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems, IEEE Transactions on Smart Grid 8 (3) (2017) 1330–1339. doi:10.1109/TSG.2016.2622289.

[71] A. Teymouri, A. Mehrizi-Sani, 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, 2018, pp. 2872–2877. doi:10.1109/IECON.2018.8591583.

[72] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, Y. Hayashi, Detection of cyber attacks against voltage control in distribution power grids with PVs, IEEE Transactions on Smart Grid 7 (4) (2016) 1824–1835. doi:10.1109/TSG.2015.2427380.

[73] H. Ibrahim, J. Kim, P. Enjeti, P. R. Kumar, L. Xie, Detection of cyber attacks in grid-tied PV systems using dynamic watermarking, in: 2022 IEEE Green Technologies Conference (GreenTech), 2022, pp. 57–61. doi:10.1109/GreenTech52845.2022.9772036.

[74] F. Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, J. Ye, W. Song, Detection and identification of cyber and physical attacks on distribution power grids with PVs: An online high-dimensional data-driven approach, IEEE Journal of Emerging and Selected Topics in Power Electronics 10 (1) (2022) 1282–1291. doi:10.1109/JESTPE.2019.2943449.

[75] Q. Li, J. Zhang, J. Ye, W. Song, Data-driven cyber-attack detection for photovoltaic systems: A transfer learning approach, in: 2022 IEEE Applied Power Electronics Conference and Exposition (APEC), 2022, pp. 1926–1930. doi:10.1109/APEC43599.2022.9773401.

[76] Q. Li, F. Li, J. Zhang, J. Ye, W. Song, A. Mantooth, Data-driven cyberattack detection for photovoltaic (PV) systems through analyzing micro-PMU data, in: 2020 IEEE Energy Conversion Congress and Exposition (ECCE), 2020, pp. 431–436. doi:10.1109/ECCE44975.2020.9236274.

[77] Renewable energy, Tech. rep., Center for Climate and Energy Solutions (2021).
URL https://www.c2es.org/content/renewable-energy/

[78] I. E. Agency, Wind power (2023).
URL https://www.iea.org/energy-system/renewables/wind

[79] Global wind report 2023, Technical report, Global Wind Energy Council (2023).
URL https://gwec.net/globalwindreport2023/

[80] Digital wind farm: The next evolution of wind energy, Tech. rep., GE Renewable Energy (2020).
URL https://www.ge.com/renewableenergy/sites/default/files/2020-01/digital-wind-farm-solutions-gea31821b-r2.pdf

[81] Digital wind cyber security from GE renewable energy, Tech. rep., General Electric (2017).
URL https://www.ge.com/digital/sites/default/files/download_assets/GE-Digital-Wind-Cyber-Security-Brochure.pdf

[82] J. Staggs, D. Ferlemann, S. Shenoi, Wind farm security: attack surface, targets, scenarios and mitigation, International journal of critical infrastructure protection 17 (2017) 3–14. doi:https://doi.org/10.1016/j.ijcip.2017.03.001.

[83] Cyber-physical resilience for wind power generation, Technical report, GE Research (2020).
URL https://www.energy.gov/sites/prod/files/2020/11/f81/CPR14_General%20Electric%20%28GE%29_Wind%20Power_2020%20CEDS%20Peer%20Review_508.pdf

[84] J. Yan, C.-C. Liu, M. Govindarasu, Cyber intrusion of wind farm SCADA system and its impact analysis, in: 2011 IEEE/PES Power Systems Conference and Exposition, 2011. doi:10.1109/PSCE.2011.5772593.

[85] Y. Zhang, Y. Xiang, L. Wang, Power system reliability assessment incorporating cyber attacks against wind farm energy management

systems, IEEE Transactions on Smart Grid 8 (5) (2017) 2343–2357. doi:10.1109/TSG.2016.2523515.

[86] H. Wu, J. Liu, J. Liu, M. Cui, X. Liu, H. Gao, Power grid reliability evaluation considering wind farm cyber security and ramping events, Applied sciences 9 (15) (2019) 3003.

[87] XZERES 442SR wind turbine vulnerability, Tech. rep., Cybersecurity & Infrastructure Security Agency (2018).
URL https://www.cisa.gov/uscert/ics/advisories/ICSA-15-076-01

[88] RLE Nova-wind turbine hmi unsecure credentials vulnerability, Tech. rep., Cybersecurity & Infrastructure Security Agency (2018).
URL https://www.cisa.gov/uscert/ics/advisories/ICSA-15-162-01A

[89] J. Johnson, J. Quiroz, R. Concepcion, F. Wilches-Bernal, M. J. Reno, Power system effects and mitigation recommendations for DER cyberattacks, IET Cyber-Physical Systems 4 (3) (2019) 240–249.

[90] X. Liu, J. Ospina, C. Konstantinou, Deep reinforcement learning for cybersecurity assessment of wind integrated power systems, IEEE Access 8 (2020) 208378–208394. doi:10.1109/ACCESS.2020.3038769.

[91] Y. Zhang, F. Lin, K. Wang, Robustness of short-term wind power forecasting against false data injection attacks, Energies (Basel) 13 (15) (2020) 3780. doi:10.3390/en13153780.

[92] W. Bi, G. Chen, K. Zhang, Profit-oriented false data injection attack against wind farms and countermeasures, IEEE Systems Journal (2021) 1–11 doi:10.1109/JSYST.2021.3107910.

[93] D. L. Marino, C. S. Wickramasinghe, V. K. Singh, J. Gentle, C. Rieger, M. Manic, The virtualized cyber-physical testbed for machine learning anomaly detection: A wind powered grid case study, IEEE Access 9 (2021) 159475–159494. doi:10.1109/ACCESS.2021.3127169.

[94] A. Amini, M. Ghafouri, A. Mohammadi, M. Hou, A. Asif, K. Plataniotis, Secure sampled-data observer-based control for wind turbine oscillation under cyber attacks, IEEE Transactions on Smart Grid 13 (4) (2022) 3188–3202. doi:10.1109/TSG.2022.3159582.

[95] M. Ghafouri, U. Karaagac, A. Ameli, J. Yan, C. Assi, A cyber attack mitigation scheme for series compensated DFIG-based wind parks, IEEE Transactions on Smart Grid 12 (6) (2021) 5221–5232. doi:10.1109/TSG.2021.3091535.

[96] A. Alassi, S. Bañales, O. Ellabban, G. Adam, C. MacIver, HVDC transmission: Technology review, market trends and future outlook, Renewable and Sustainable Energy Reviews 112 (2019) 530–554. doi:https://doi.org/10.1016/j.rser.2019.04.062.
URL https://www.sciencedirect.com/science/article/pii/S1364032119302837

[97] M. Intelligence, HVDC transmission systems market - growth, trends, COVID-19 impact, and forecasts (2023 - 2028), Tech. rep., Mordor

Intelligence (2023).
URL https://www.mordorintelligence.com/industry-reports/global-hvdc-transmission-systems-market-industry

[98] ABB review special report - 60 years of HVDC, Tech. rep., ABB (2014).
URL https://library.e.abb.com/public/aff841e25d8986b5c1257d380045703f/140818%20ABB%20SR%2060%20years%20of%20HVDC_72dpi.pdf

[99] M. A. Elizondo, R. Fan, H. Kirkham, M. Ghosal, F. Wilches-Bernal, D. Schoenwald, J. Lian, Interarea oscillation damping control using high-voltage dc transmission: A survey, IEEE Transactions on Power Systems 33 (6) (2018) 6915–6923. doi:10.1109/TPWRS.2018.2832227.

[100] R. Dai, G. Liu, X. Zhang, Transmission technologies and implementations: Building a stronger, smarter power grid in China, IEEE Power and Energy Magazine 18 (2) (2020) 53–59. doi:10.1109/MPE.2019.2957623.

[101] D. Roberson, H. C. Kim, B. Chen, C. Page, R. Nuqui, A. Valdes, R. Macwan, B. K. Johnson, Improving grid resilience using high-voltage dc: Strengthening the security of power system stability, IEEE Power and Energy Magazine 17 (3) (2019) 38–47. doi:10.1109/MPE.2019.2897407.

[102] PD IEC TR 60919-1:2020: Performance of high-voltage direct current (HVDC) systems with line-commutated converters. steady-state conditions (2020).

[103] PD IEC TR 62543:2011+a2:2017: High-voltage direct current (HVDC) power transmission using voltage sourced converters (VSC) (2017).

[104] J. Binkai, W. Zhixin, The key technologies of VSC-MTDC and its application in China, Renewable and Sustainable Energy Reviews 62 (2016) 297–304. doi:https://doi.org/10.1016/j.rser.2016.04.067.
URL https://www.sciencedirect.com/science/article/pii/S1364032116301009

[105] D. Van Hertem, W. Leterme, G. Chaffey, M. Abedrabbo, M. Wang, F. Zerihun, M. Barnes, Substations for future HVdc grids: Equipment and configurations for connection of HVdc network elements, IEEE Power and Energy Magazine 17 (4) (2019) 56–66. doi:10.1109/MPE.2019.2909006.

[106] Introduction to HVDC architecture and solutions for control and protection, Application report, Texas Instruments (2021).
URL https://www.ti.com/lit/an/sloa289b/sloa289b.pdf?ts=1656421028367&ref_url=https%253A%252F%252F%252F

[107] Cyber security services HVDC and FACTS, Tech. rep., Hitachi Energy (2021).
URL https://search.abb.com/library/Download.aspx?DocumentID=9AKK107680A8598&LanguageCode=en&DocumentPartId=&Action=Launch

[108] Cyber security for HVDC & FACTS - cyber security services, Tech. rep., Siemens Energy (2021).

URL https://assets.siemens-energy.com/siemens/assets/api/uuid:2ec35f7e-6264-4c33-a857-08cfddb53d08/se-ff-en-cyber-security.pdf

[109] T. Ding, Z. Zeng, B. Qin, J. Zhao, Y. Yang, F. Blaabjerg, Z. Dong, Quantifying cyber attacks on industrial MMC-HVDC control system using structured pseudospectrum, IEEE Transactions on Power Electronics 36 (5) (2021) 4915–4920. doi:10.1109/TPEL.2020.3032883.

[110] Y. Zhao, W. Yao, C.-K. Zhang, X.-C. Shangguan, L. Jiang, J. Wen, Quantifying resilience of wide-area damping control against cyber attack based on switching system theory, IEEE Transactions on Smart Grid 13 (3) (2022) 2331–2343. doi:10.1109/TSG.2022.3146375.

[111] R. Fan, J. Lian, K. Kalsi, M. Elizondo, Impact of cyber attacks on high voltage dc transmission damping control, Energies (Basel) 11 (5) (2018) 1046. doi:10.3390/en11051046.

[112] K. Pan, J. Dong, E. Rakhshani, P. Palensky, Effects of cyber attacks on ac and high-voltage dc interconnected power systems with emulated inertia, Energies 13 (21) (2020). doi:10.3390/en13215583.
URL https://www.mdpi.com/1996-1073/13/21/5583

[113] R. Nuqui, H. Lee, A. Kondabathini, M. Overeem, J. Barton, Cyber secured power orders for resilient HVDC systems, in: 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), 2020, pp. 1–5. doi:10.1109/TD39804.2020.9299994.

[114] J. Hatton, B. K. Johnson, D. Roberson, R. Nuqui, Increased grid resilience via cyber-secure VSC multiterminal HVDC systems, in: 2019 IEEE Power & Energy Society General Meeting (PESGM), 2019. doi:10.1109/PESGM40551.2019.8973937.

[115] C. L. Page, B. K. Johnson, D. Roberson, R. Nuqui, Increasing grid resilience via cyber-secure series multiterminal LCC HVDC transmission systems, in: 2020 52nd North American Power Symposium (NAPS), 2021. doi:10.1109/NAPS50074.2021.9449720.

[116] K. Sun, W. Qiu, W. Yao, S. You, H. Yin, Y. Liu, Frequency injection based HVDC attack-defense control via squeeze-excitation double CNN, IEEE Transactions on Power Systems 36 (6) (2021) 5305–5316. doi:10.1109/TPWRS.2021.3078770.

[117] S. D. Roy, S. Debbarma, J. M. Guerrero, Machine learning based multi-agent system for detecting and neutralizing unseen cyber-attacks in AGC and HVDC systems, IEEE Journal on Emerging and Selected Topics in Circuits and Systems 12 (1) (2022) 182–193. doi:10.1109/JETCAS.2022.3142055.

[118] B. Chen, S.-i. Yim, H. C. Kim, R. Nuqui, Cyber attack detection for WAMPAC-based HVDC applications, in: 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), 2020. doi:10.1109/TD39804.2020.9299662.

[119] W. Qiu, K. Sun, W. Yao, W. Wang, Q. Tang, Y. Liu, Hybrid data-driven based HVdc ancillary control for multiple frequency data attacks,

IEEE Transactions on Industrial Informatics 17 (12) (2021) 8035–8045. doi:10.1109/TII.2021.3063270.

[120] W. Yao, J. Nan, Y. Zhao, J. Fang, X. Ai, W. Zuo, J. Wen, S. Cheng, Resilient wide-area damping control for inter-area oscillations to tolerate deception attacks, IEEE Transactions on Smart Grid 12 (5) (2021) 4238–4249. doi:10.1109/TSG.2021.3068390.

[121] Y. Zhao, W. Yao, J. Nan, J. Fang, X. Ai, J. Wen, S. Cheng, Resilient adaptive wide-area damping control to mitigate false data injection attacks, IEEE Systems Journal 15 (4) (2021) 4831–4842. doi:10.1109/JSYST.2020.3020425.

[122] K. Sun, W. Qiu, Y. Dong, C. Zhang, H. Yin, W. Yao, Y. Liu, WAMS-based HVDC damping control for cyber attack defense, IEEE Transactions on Power Systems (2022) 1–1 doi:10.1109/TPWRS.2022.3168078.

[123] J. Hou, S. Lei, W. Yin, W. Sun, Y. Hou, Cybersecurity enhancement for multi-infeed high-voltage dc systems, IEEE Transactions on Smart Grid 13 (4) (2022) 3227–3240. doi:10.1109/TSG.2022.3156796.

[124] Global EV outlook 2022, Tech. rep., International Energy Agency (IEA) (2022).
URL https://www.iea.org/reports/global-ev-outlook-2022

[125] BloombergNEF, Electric vehicle outlook 2022 (2022).
URL https://about.bnef.com/electric-vehicle-outlook

[126] C. Hodge, K. Hauck, S. Gupta, J. C. Bennett, Vehicle cybersecurity threats and mitigation approaches, Tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States) (2019).

[127] ICS-CERT advisories - schneider electric evlink parking, Tech. rep., Schneider Electric (2018).
URL https://us-cert.cisa.gov/ics/advisories/ICSA-19-031-01

[128] R. M. Pratt, F. K. Tuffner, K. Gowri, Electric vehicle communication standards testing and validation phase i: SAE J2847/1, Tech. rep., Pacific Northwest National Lab (2011). doi:10.2172/1126382.
URL https://www.osti.gov/biblio/1126382

[129] Consequence-driven cybersecurity for high-power EV charging infrastructure, Tech. rep., Idaho National Laboratory (2021).
URL https://www.energy.gov/sites/default/files/2021-06/elt199_carlson_2021_o_5-12_351pm_LR_TM.pdf

[130] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, W. Song, Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions, IEEE Journal of Emerging and Selected Topics in Power Electronics 9 (4) (2020) 4639–4657. doi:10.1109/JESTPE.2020.3045667.

[131] K. Harnett, B. Harris, D. Chin, G. Watson, et al., DOE/DHS/DOT volpe technical meeting on electric vehicle and charging station cybersecurity report, Tech. rep., John A. Volpe National Transportation

Systems Center (US) (2018).
URL https://rosap.ntl.bts.gov/view/dot/34991

[132] H. Olufowobi, G. Bloom, Chapter 16 - connected cars: Automotive cybersecurity and privacy for smart cities, in: D. B. Rawat, K. Z. Ghafoor (Eds.), Smart Cities Cybersecurity and Privacy, Elsevier, 2019, pp. 227–240. doi:https://doi.org/10.1016/B978-0-12-815032-0.00016-0.
URL https://www.sciencedirect.com/science/article/pii/B9780128150320000160

[133] H. Li, D. Han, M. Tang, A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing, IEEE Systems Journal 15 (3) (2021) 3189–3200. doi:10.1109/JSYST.2020.3009447.

[134] S. Dey, A. Chandwani, A. Mallik, Real time intelligent data processing algorithm for cyber resilient electric vehicle onboard chargers, in: 2021 IEEE Transportation Electrification Conference & Expo (ITEC), 2021, pp. 1–6. doi:10.1109/ITEC51675.2021.9490067.

[135] W. Wang, Z. Han, M. Alazab, T. R. Gadekallu, X. Zhou, C. Su, Ultra super fast authentication protocol for electric vehicle charging using extended chaotic maps, IEEE Transactions on Industry Applications (2022) 1–8 doi:10.1109/TIA.2022.3184668.

[136] S. Acharya, Y. Dvorkin, R. Karri, Public plug-in electric vehicles + grid data: Is a new cyberattack vector viable?, IEEE Transactions on Smart Grid 11 (6) (2020) 5099–5113. doi:10.1109/TSG.2020.2994177.

[137] L. Guo, J. Ye, Cyber-physical security of electric vehicles with four motor drives, IEEE Transactions on Power Electronics 36 (4) (2021) 4463–4477. doi:10.1109/TPEL.2020.3025718.

[138] S. Dey, M. Khanra, Cybersecurity of plug-in electric vehicles: Cyberattack detection during charging, IEEE Transactions on Industrial Electronics 68 (1) (2021) 478–487. doi:10.1109/TIE.2020.2965497.

[139] M. Girdhar, J. Hong, H. Lee, T.-j. Song, Hidden markov models based anomaly correlations for the cyber-physical security of EV charging stations, IEEE Transactions on Smart Grid (2021) 1–1 doi:10.1109/TSG.2021.3122106.

[140] Z. Abdollahi Biron, S. Dey, P. Pisu, Real-time detection and estimation of denial of service attack in connected vehicle systems, IEEE Transactions on Intelligent Transportation Systems 19 (12) (2018) 3893–3902. doi:10.1109/TITS.2018.2791484.

[141] A. Kavousi-Fard, M. Dabbaghjamanesh, T. Jin, W. Su, M. Roustaei, An evolutionary deep learning-based anomaly detection model for securing vehicles, IEEE Transactions on Intelligent Transportation Systems 22 (7) (2021) 4478–4486. doi:10.1109/TITS.2020.3015143.

[142] M. M. Rana, IoT-based electric vehicle state estimation and control algorithms under cyber attacks, IEEE Internet of Things Journal 7 (2) (2020) 874–881. doi:10.1109/JIOT.2019.2946093.

[143] S. Mousavian, M. Erol-Kantarci, L. Wu, T. Ortmeyer, A risk-based optimization model for electric vehicle infrastructure response to cyber

attacks, IEEE Transactions on Smart Grid 9 (6) (2018) 6160–6169. doi:10.1109/TSG.2017.2705188.

[144] M. E. Kabir, M. Ghafouri, B. Moussa, C. Assi, A two-stage protection method for detection and mitigation of coordinated EVSE switching attacks, IEEE Transactions on Smart Grid 12 (5) (2021) 4377–4388. doi:10.1109/TSG.2021.3083696.

[145] G. A. f. B. United Nations Environment Programme, Construction, 2020 global status report for buildings and construction: Towards a zero-emissions, efficient and resilient buildings and construction sector - executive summary (2020).
URL https://wedocs.unep.org/20.500.11822/34572

[146] H. Song, G. A. Fink, S. Jeschke, Security and privacy in cyber-physical systems: foundations, principles, and applications, John Wiley & Sons, 2017.

[147] Challenges and opportunities to secure buildings from cyber threats, Tech. rep., Pacific Northwest National Laboratory (2020).
URL https://www.energy.gov/eere/buildings/articles/challenges-and-opportunities-secure-buildings-cyber-threats

[148] M. Neukomm, V. Nubbe, R. Fares, Grid-interactive efficient buildings technical report series: Overview of research challenges and gaps, Tech. rep., National Renewable Energy Lab.(NREL), Golden, CO (United States) (2019). doi:10.2172/1577966.
URL https://www.osti.gov/biblio/1577966

[149] S. Wendzel, J. Tonejc, J. Kaur, A. Kobekova, H. Song, G. Fink, S. Jeschke, Cyber security of smart buildings, Wiley, 2017.

[150] K. Kruglov, Threat landscape for smart buildings (2019). URL https://securelist.com/smart-buildings-threats/93322/

[151] Y. Fu, Z. O'Neill, V. Adetola, A flexible and generic functional mock-up unit based threat injection framework for grid-interactive efficient buildings: A case study in modelica, Energy and Buildings 250 (2021) 111263. doi:https://doi.org/10.1016/j.enbuild.2021.111263.

[152] D. Meyer, J. Haase, M. Eckert, B. Klauer, A threat-model for building and home automation, in: 2016 IEEE 14th International Conference on Industrial Informatics (INDIN), 2016, pp. 860–866. doi:10.1109/INDIN.2016.7819280.

[153] A. Sheikh, V. Kamuni, A. Patil, S. Wagh, N. Singh, Cyber attack and fault identification of HVAC system in building management systems, in: 2019 9th International Conference on Power and Energy Systems (ICPES), 2019, pp. 1–6. doi:10.1109/ICPES47639.2019.9105438.

[154] Y. Fu, Z. O'Neill, Z. Yang, V. Adetola, J. Wen, L. Ren, T. Wagner, Q. Zhu, T. Wu, Modeling and evaluation of cyber-attacks on grid-interactive efficient buildings, Applied Energy 303 (2021) 117639. doi:https://doi.org/10.1016/j.apenergy.2021.117639.

[155] K. Paridari, A. E.-D. Mady, S. La Porta, R. Chabukswar, J. Blanco, A. Teixeira, H. Sandberg, M. Boubekeur, Cyber-physical-security frame-

work for building energy management system, in: 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), 2016, pp. 1–9. doi:10.1109/ICCPS.2016.7479072.

[156] S. Xu, Y. Fu, Y. Wang, Z. O'Neill, Q. Zhu, Learning-based framework for sensor fault-tolerant building HVAC control with model-assisted learning, in: Proceedings of the 8th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation, 2021. doi:10.1145/3486611.3486644.

[157] D. T. Ton, M. A. Smith, The U.S. department of energy's microgrid initiative, The Electricity Journal 25 (8) (2012) 84–94. doi:https://doi.org/10.1016/j.tej.2012.09.013.
URL https://www.sciencedirect.com/science/article/pii/S1040619012002254

[158] N. Priyadharshini, S. Gomathy, M. Sabarimuthu, A review on microgrid architecture, cyber security threats and standards, Materials Today: Proceedings (2020).

[159] L. Marinos, ENISA threat taxonomy: A tool for structuring threat information, ENISA, Heraklion (2016).
URL https://www.um.es/documents/2096502/4937674/Enisa.pdf/2374a6a9-3c9d-422c-b5ad-b047a2fb8568

[160] D. P. Duggan, S. R. Thomas, C. K. Veitch, L. Woodard, Categorizing threat: Building and using a generic threat matrix, Sandia National

Laboratories report SAND2007-5791, Albuquerque, New Mexico (2007). doi:10.2172/921121.

[161] B. Canaan, B. Colicchio, D. Ould Abdeslam, Microgrid cyber-security: Review and challenges toward resilience, Applied Sciences 10 (16) (2020) 5649. doi:10.3390/app10165649.

[162] IEEE recommended practice for the planning and design of the microgrid, IEEE Std 2030.9-2019 (2019) 1–46 doi:10.1109/IEEESTD.2019.8746836.

[163] J. Zhang, S. Sahoo, J. C.-H. Peng, F. Blaabjerg, Mitigating concurrent false data injection attacks in cooperative dc microgrids, IEEE Transactions on Power Electronics 36 (8) (2021) 9637–9647. doi:10.1109/TPEL.2021.3055215.

[164] N. Nikmehr, S. Moradi Moghadam, Game-theoretic cybersecurity analysis for false data injection attack on networked microgrids, IET Cyber-Physical Systems: Theory & Applications 4 (4) (2019) 365–373.

[165] A. S. Mohamed, M. F. M. Arani, A. A. Jahromi, D. Kundur, False data injection attacks against synchronization systems in microgrids, IEEE Transactions on Smart Grid 12 (5) (2021) 4471–4483. doi:10.1109/TSG.2021.3080693.

[166] A. Saad, S. Faddel, T. Youssef, O. A. Mohammed, On the implementation of IoT-based digital twin for networked microgrids resiliency against cyber attacks, IEEE Transactions on Smart Grid 11 (6) (2020) 5138–5150. doi:10.1109/TSG.2020.3000958.

[167] J. Hao, E. Kang, J. Sun, Z. Wang, Z. Meng, X. Li, Z. Ming, An adaptive markov strategy for defending smart grid false data injection from malicious attackers, IEEE Transactions on Smart Grid 9 (4) (2018) 2398–2408. doi:10.1109/TSG.2016.2610582.

[168] M. R. Khalghani, J. Solanki, S. K. Solanki, M. H. Khooban, A. Sargolzaei, Resilient frequency control design for microgrids under false data injection, IEEE Transactions on Industrial Electronics 68 (3) (2021) 2151–2162. doi:10.1109/TIE.2020.2975494.

[169] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, J. Zhang, A FDI attack-resilient distributed secondary control strategy for islanded microgrids, IEEE Transactions on Smart Grid 12 (3) (2021) 1929–1938. doi:10.1109/TSG.2020.3047949.

[170] Y. Liu, Y. Li, Y. Wang, X. Zhang, H. B. Gooi, H. Xin, Robust and resilient distributed optimal frequency control for microgrids against cyber attacks, IEEE Transactions on Industrial Informatics 18 (1) (2022) 375–386. doi:10.1109/TII.2021.3071753.

[171] M. Chlela, D. Mascarella, G. Joós, M. Kassouf, Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks, IEEE Transactions on Smart Grid 9 (5) (2018) 4702–4711. doi:10.1109/TSG.2017.2667586.

[172] H. Zhou, W. Xu, J. Chen, W. Wang, Evolutionary V2X technologies toward the internet of vehicles: Challenges and opportunities, Proceed-

ings of the IEEE 108 (2) (2020) 308–323. doi:10.1109/JPROC.2019.2961937.

[173] P. Ciholas, A. Lennie, P. Sadigova, J. M. Such, The security of smart buildings: a systematic literature review, arXiv preprint arXiv:1901.05837 (2019).

[174] China electric vehicle and connected vehicle security and privacy, Tech. rep., The Fraunhofer Institute for Secure Information Technology (SIT) (2021).
URL https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/China-electric-vehicle-study_2021.pdf

[175] B. Tarekegne, R. O'Neil, J. Twitchell, Energy storage as an equity asset, Current Sustainable/Renewable Energy Reports 8 (3) (2021) 149–155. doi:https://doi.org/10.1007/s40518-021-00184-6.

[176] E. S. G. Challenge, Energy storage market report, US Department of Energy: December (2020).
URL https://www.energy.gov/sites/prod/files/2020/12/f81/Energy%20Storage%20Market%20Report%202020_0.pdf

[177] G. A. Francia III, E. El-Sheikh, NERC CIP standards: Review, compliance, and training, Tech. rep., North American Electric Reliability Corporation (NERC) (2022). doi:10.4018/978-1-7998-8390-6.ch003.

[178] IEEE guide for the interoperability of energy storage systems integrated

with the electric power infrastructure, IEEE Std 2030.2-2015 (2015) 1–138 doi:10.1109/IEEESTD.2015.7140715.

[179] Standard for the installation of stationary energy storage systems, Tech. rep., National Fire Protection Association (NFPA) (2018).
URL https://www.aft.net/wp-content/uploads/2018/10/ESS-NFPA-855.pdf

[180] D. R. Conover, P. Cole, DOE OE energy storage systems safety roadmap focus on codes and standards may 2018 (5 2018). doi:10.2172/1761963.
URL https://www.osti.gov/biblio/1761963

[181] P. Zhuang, H. Liang, False data injection attacks against state-of-charge estimation of battery energy storage systems in smart distribution networks, IEEE Transactions on Smart Grid 12 (3) (2021) 2566–2577. doi:10.1109/TSG.2020.3042926.

[182] M. Pasetti, P. Ferrari, P. Bellagente, E. Sisinni, A. O. de Sá, C. B. d. Prado, R. P. David, R. C. S. Machado, Artificial neural network-based stealth attack on battery energy storage systems, IEEE Transactions on Smart Grid 12 (6) (2021) 5310–5321. doi:10.1109/TSG.2021.3102833.

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

Energy Conversion 36 (4) (2021) 3108–3117. doi:10.1109/TEC.2021.3061493.

[184] A. Farraj, E. Hammad, D. Kundur, On the impact of cyber attacks on data integrity in storage-based transient stability control, IEEE Transactions on Industrial Informatics 13 (6) (2017) 3322–3333. doi:10.1109/TII.2017.2720679.

[185] L. Ding, Q.-L. Han, B. Ning, D. Yue, Distributed resilient finite-time secondary control for heterogeneous battery energy storage systems under denial-of-service attacks, IEEE Transactions on Industrial Informatics 16 (7) (2020) 4909–4919. doi:10.1109/TII.2019.2955739.

[186] P. Chen, S. Liu, B. Chen, L. Yu, Multi-agent reinforcement learning for decentralized resilient secondary control of energy storage systems against dos attacks, IEEE Transactions on Smart Grid 13 (3) (2022) 1739–1750. doi:10.1109/TSG.2022.3142087.

[187] C. Deng, Y. Wang, C. Wen, Y. Xu, P. Lin, Distributed resilient control for energy storage systems in cyber–physical microgrids, IEEE Transactions on Industrial Informatics 17 (2) (2021) 1331–1341. doi:10.1109/TII.2020.2981549.

[188] D. D. Sharma, S. N. Singh, J. Lin, E. Foruzan, Agent-based distributed control schemes for distributed energy storage systems under cyber attacks, IEEE Journal on Emerging and Selected Topics in Circuits and Systems 7 (2) (2017) 307–318. doi:10.1109/JETCAS.2017.2700947.

[189] A. Abur, Power system state estimation : theory and implementation, Power engineering ; 24, Marcel Dekker, New York, 2004.

[190] J. Hou, S. Lei, Y. Song, L. Zhu, W. Sun, Y. Hou, The cost and benefit of enhancing cybersecurity for hybrid ac/dc grids, IEEE Transactions on Smart Grid (2023) 1–1 doi:10.1109/TSG.2023.3255250.

[191] A. Gopstein, N. Hastings, L. Feldman, R. Agarwal, N. Bartol, et al., Distributed energy resource security: Potential guidelines and research topics (NIST 2182) (2021). doi:https://doi.org/10.6028/NIST.TN.2182.

[192] X. Liu, Z. Li, Local load redistribution attacks in power systems with incomplete network information, IEEE Transactions on Smart Grid 5 (4) (2014) 1665–1676. doi:10.1109/TSG.2013.2291661.

[193] H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung, Y. Zhang, C.-K. Wen, Local cyber-physical attack for masking line outage and topology attack in smart grid, IEEE Transactions on Smart Grid 10 (4) (2019) 4577–4588. doi:10.1109/TSG.2018.2865316.

[194] J. Hou, J. Wang, Y. Song, W. Sun, Y. Hou, Small-signal angle stability-oriented false data injection cyber-attacks on power systems, IEEE Transactions on Smart Grid 14 (1) (2023) 635–648. doi:10.1109/TSG.2022.3199366.

[195] Y. Liu, P. Ning, M. K. Reiter, False data injection attacks against state estimation in electric power grids, ACM Transactions on Informa-

tion and System Security 14 (1) (2011) 1–33. doi:10.1145/1952982.1952995.

[196] C. Liu, M. Zhou, J. Wu, C. Long, D. Kundur, Financially motivated FDI on SCED in real-time electricity markets: Attacks and mitigation, IEEE Transactions on Smart Grid 10 (2) (2019) 1949–1959. doi:10.1109/TSG.2017.2784366.

[197] Cyber intrusion guide for system operators (version 2), Tech. rep., North American Electric Reliability Corporation (NERC) (2018). URL https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline-Cyber_Intrusion_Guide_for_System_Operators.pdf

[198] ISO/IEC 27000—key international standard for information security revised, Tech. rep., International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2018).

[199] IEEE standard cybersecurity requirements for substation automation, protection, and control systems, IEEE Std C37.240-2014 (2015) 1–38 doi:10.1109/IEEESTD.2015.7024885.

[200] Wind energy generation systems - part 25-1: Communications for monitoring and control of wind power plants - overall description of principles and models, IEC 61400-25-1:2017 (2017) 1–73.

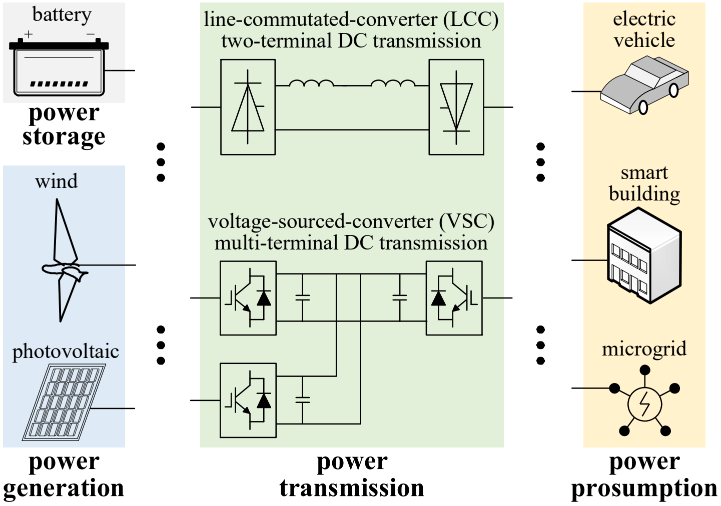


Figure. 1: A power electronics-enabled power system with power electronics devices in power generation, power transmission, power prosumption, and power storage.

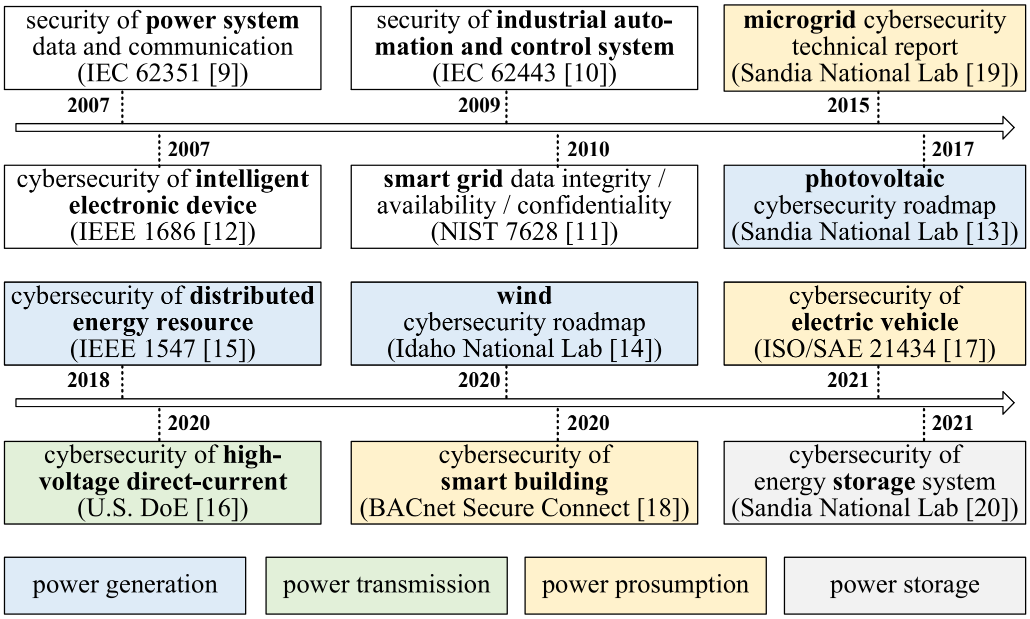

security of power system data and communication (IEC 62351 [9])
2007
security of industrial automation and control system (IEC 62443 [10])
2009
microgrid cybersecurity technical report (Sandia National Lab [19])
2015
2007
cybersecurity of intelligent electronic device (IEEE 1686 [12])
2010
smart grid data integrity / availability / confidentiality (NIST 7628 [11])
2017
photovoltaic cybersecurity roadmap (Sandia National Lab [13])
cybersecurity of distributed energy resource (IEEE 1547 [15])
2018
wind cybersecurity roadmap (Idaho National Lab [14])
2020
cybersecurity of electric vehicle (ISO/SAE 21434 [17])
2021
2020
cybersecurity of high-voltage direct-current (U.S. DoE [16])
2020
cybersecurity of smart building (BACnet Secure Connect [18])
2021
cybersecurity of energy storage system (Sandia National Lab [20])
power generation
power transmission
power prosumption
power storage

Figure. 2: A timeline of representative regulations and roadmaps of power systems and power electronics devices. BACnet: Building Autmoation and Control network. DoE: Department of Energy. IEC: International Organization for Standardization. NIST: National Institute of Standards and Technology. SAE: Society of Automotive Engineers.

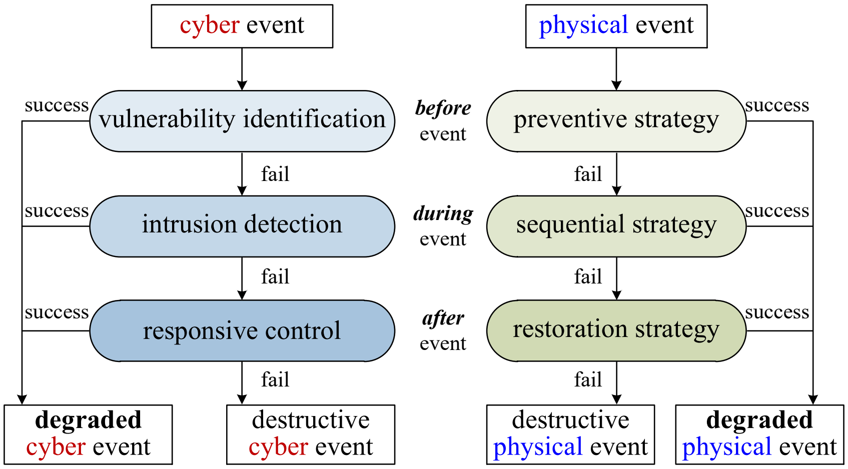


Figure. 3: Cyber or physical resilience before, during, and after a cyber or physical event.

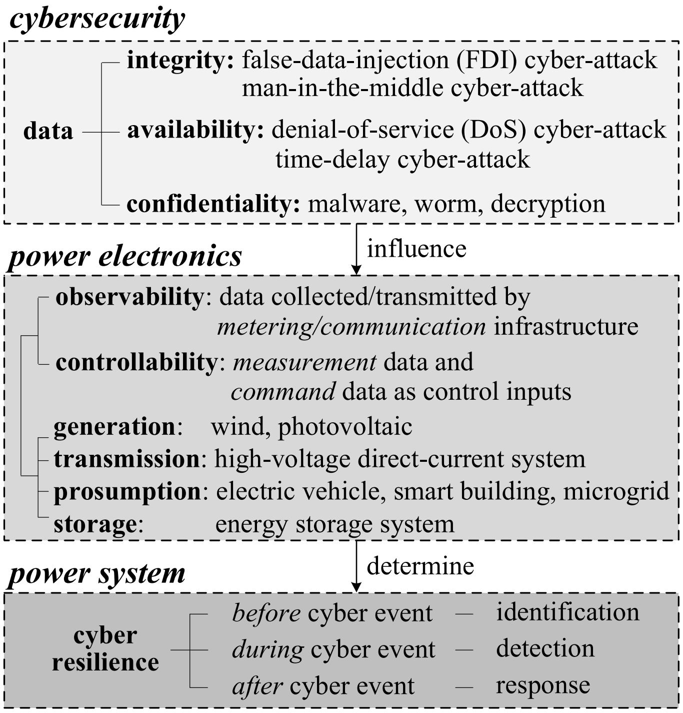

cybersecurity
data
integrity: false-data-injection (FDI) cyber-attack
man-in-the-middle cyber-attack
availability: denial-of-service (DoS) cyber-attack
time-delay cyber-attack
confidentiality: malware, worm, decryption
influence
power electronics
observability: data collected/transmitted by
metering/communication infrastructure
controllability: measurement data and
command data as control inputs
generation: wind, photovoltaic
transmission: high-voltage direct-current system
prosumption: electric vehicle, smart building, microgrid
storage: energy storage system
determine
power system
cyber resilience
before cyber event – identification
during cyber event – detection
after cyber event – response

Figure. 4: Three interdependent research fields in investigating the cyber resilience of a power electronics-enabled power system.

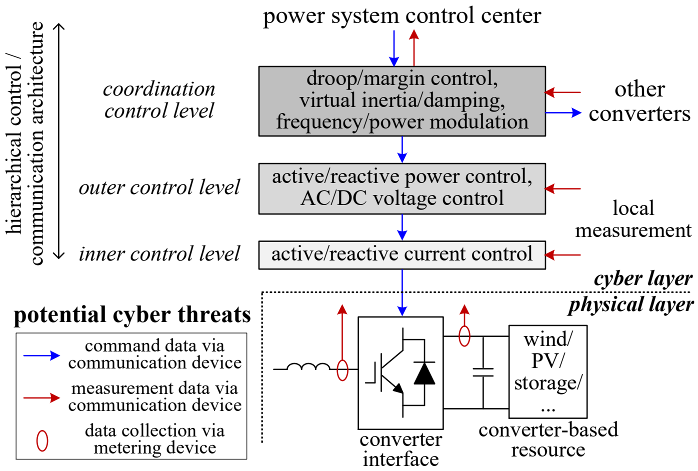


Figure. 5: Control and communication architecture of a grid-tied converter.

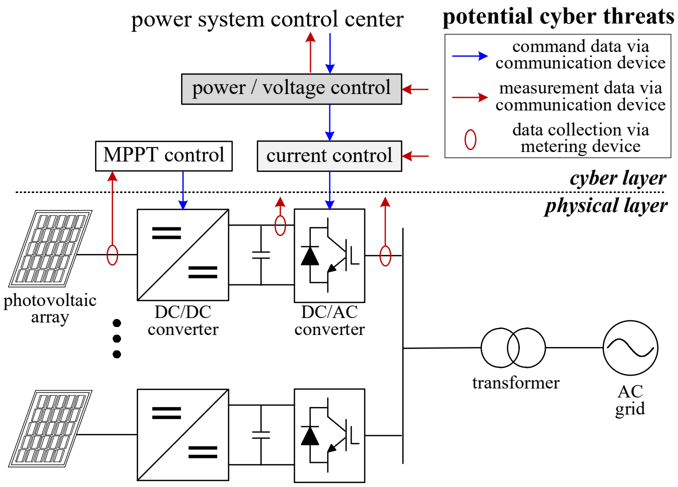


Figure. 6: Control and communication architecture of a typical photovoltaic system. MPPT: maximum power point tracking.

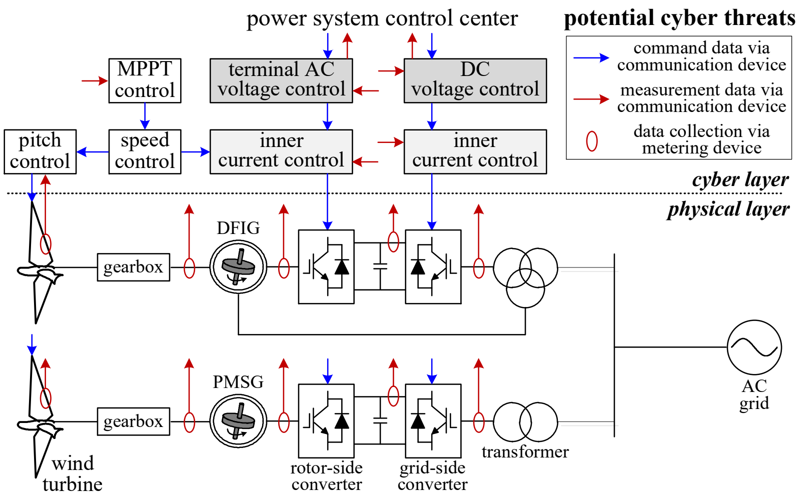


Figure. 7: Control and communication architecture of the doubly-fed induction generator (DFIG) wind generation and the permanent magnet synchronous generator (PMSG) wind generation. MPPT: maximum power point tracking.

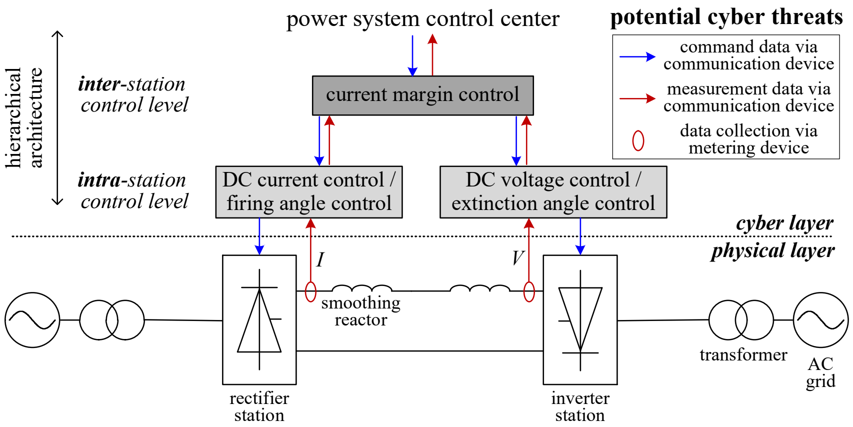

power system control center
potential cyber threats
command data via communication device
measurement data via communication device
data collection via metering device
hierarchical architecture
inter-station control level
intra-station control level
current margin control
DC current control / firing angle control
DC voltage control / extinction angle control
cyber layer
physical layer
I
V
smoothing reactor
rectifier station
inverter station
transformer
AC grid

Figure. 8: Control and communication architecture of a two-terminal LCC HVDC system.

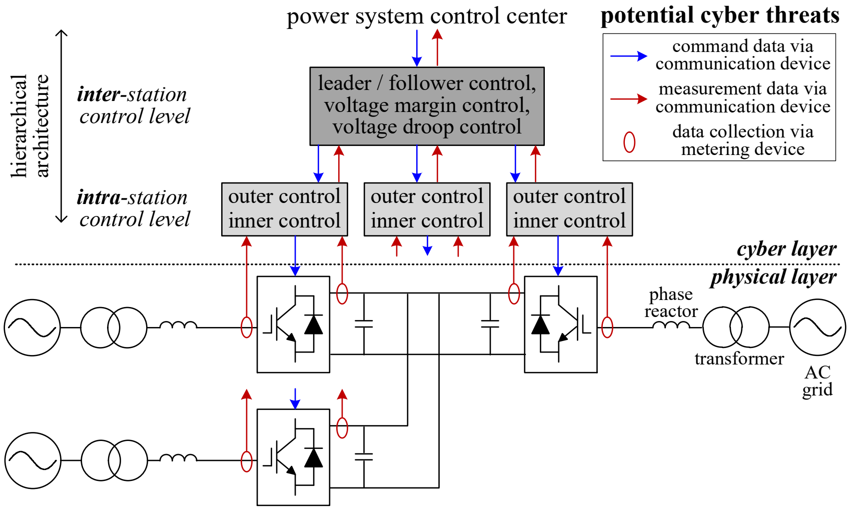

power system control center
potential cyber threats
command data via communication device
measurement data via communication device
data collection via metering device
hierarchical architecture
inter-station control level
intra-station control level
leader / follower control, voltage margin control, voltage droop control
outer control
inner control
outer control
inner control
outer control
inner control
cyber layer
physical layer
phase reactor
transformer
AC grid

Figure. 9: Control and communication architecture of a multi-terminal VSC HVDC system.

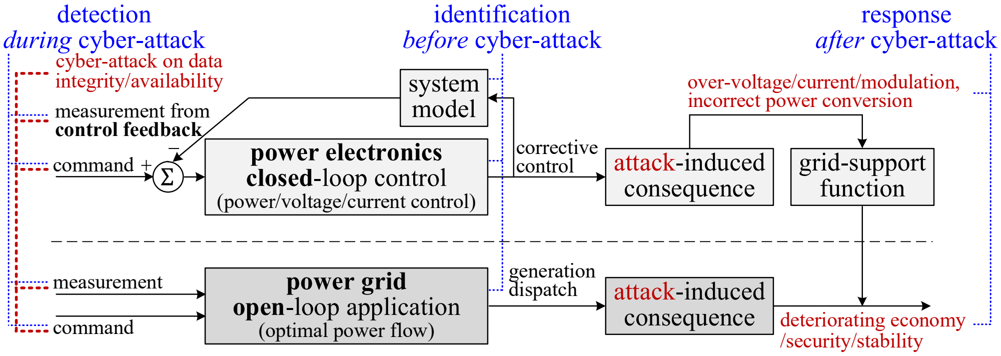

detection
during cyber-attack
identification
before cyber-attack
response
after cyber-attack
cyber-attack on data integrity/availability
measurement from **control feedback**
command
+
−
Σ
system model
power electronics
closed-loop control
(power/voltage/current control)
corrective control
attack-induced consequence
grid-support function
over-voltage/current/modulation, incorrect power conversion
measurement
command
power grid
open-loop application
(optimal power flow)
generation dispatch
attack-induced consequence
deteriorating economy /security/stability

Figure. 10: Comparison of the cyber attack/defense paradigms between the power electronics closed-loop control and the power grid open-loop application.