1

Introduction

1.1 Renewable-intensive Power Grids

1.1.1 Inverter Interfaces

The electric power grid is among the most complex engineered systems ever constructed. It is critical for modern economic and social activity. Historically, electricity has been produced predominantly by burning fossil fuels. This paradigm has been identified as a principal driver of anthropogenic climate change. In response, many countries have issued national and sectoral roadmaps to achieve carbon neutrality within the coming decades.

As a central pillar of these roadmaps, legacy power systems are undergoing a rapid transition. As illustrated in Figure 1.1, the power generation portfolio is shifting from large synchronous machines toward high penetration of renewable resources such as wind and photovoltaics (PV). On the demand side, traditional induction motor loads are giving way to a heterogeneous collection of digitally connected, interactive devices, including electric vehicles (EVs), smart buildings, and microgrids. In addition, both the supply and demand sides increasingly deploy grid-scale energy storage to buffer variability and maintain power balance. Finally, to support long-distance bulk-power delivery from resource-rich regions to load centers, transmission systems increasingly employ high-voltage direct-current (HVDC) links alongside conventional alternating current (AC) corridors.

These developments are enabled by power electronics devices, which are embedded throughout the power grid to achieve high-efficiency energy utilization and control. Moreover, interconnection of these devices to the main AC grid requires *inverters* to achieve efficient and controllable power conversion. As a result, traditional synchronous-machine-based power grids are steadily evolving into *inverter-interfaced power grids*, in which the aggregate behavior is increasingly shaped by the controls of billions of converter interfaces rather than the electromechanical properties of rotating machines.

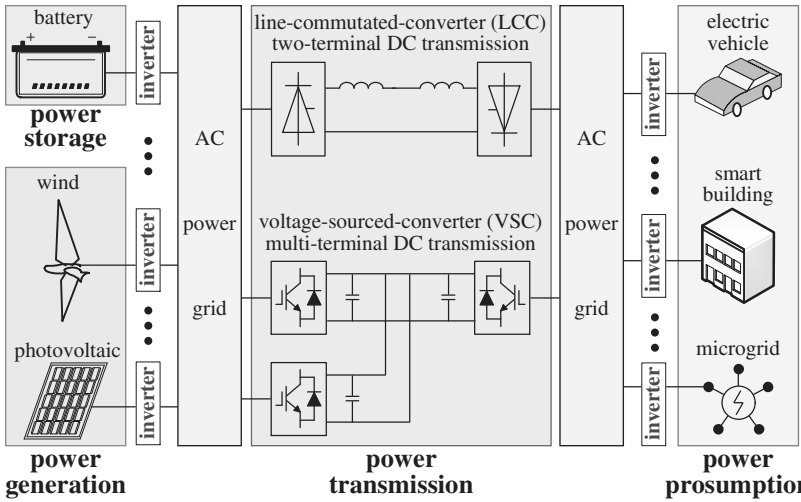

Figure 1.1 Inverter-interfaced power grids with power electronics devices in power generation, power transmission, power prosumption, and power storage.

1.1.2 Cyber Threats

The power grid is a critical infrastructure whose reliable operation depends on robust industrial control systems and supervisory control and data acquisition architectures. It is also an exceptionally complex cyber-physical system: secure physical operation hinges on the real-time collection, transmission, and processing of vast quantities of data by the underlying cyber infrastructure. Faults or compromises at any point in this information chain can propagate to the physical layer and precipitate operational disruptions. This cyber-physical interdependence simultaneously increases the likelihood of adverse events and lowers the barrier to malicious interference, rendering modern power grids *inherently vulnerable* to cyberattacks.

Prominent incidents underscore this risk. In 2015 and 2016, cyberattacks on the Ukrainian power grid compromised dozens of substations, interrupting service to approximately 225,000 customers for several hours. Particularly for inverter-interfaced grids, the proliferation of power-electronic assets introduces a large number of geographically dispersed cyber-physical access points, further amplifying system-wide cyber risk. Table 1.1 compiles representative incidents across power-electronic assets. For *generation* devices, more than 100 MW PV plant experienced a denial-of-service attack on its firewall, and roughly 500 MW of wind turbines were compromised via intrusions into the operator's control system. For *prosumption* devices, connected vehicles have been shown vulnerable: researchers remotely controlled a Tesla's steering and interfered with its automatic wipers, and

Table 1.1 Representative cyber-attack events on power electronics devices in power systems.

Device	Description	Location and time
Generation (photovoltaic)	Over a 100 MW PV project was compromised by a denial-of-service cyber-attack on the firewall [1]	US 2021
Generation (wind)	Around 500 MW of wind turbines were compromised by cyberattacks on the wind operator's control system [2]	US 2019
Prosumption (electric vehicle)	Researchers remotely controlled Tesla's steering system and disturbed the auto-wiper function [3]	China 2019
	Researchers remotely controlled a Jeep Cherokee, shunted down its acceleration, and disabled its brakes [4]	US 2015
Prosumption (smart building)	Target corporation was hacked via HVAC systems, leading to the leakage of 40 million debit and credit card accounts [5]	US 2019
	The building management system of Google Australia Office was hacked by researchers [6]	Australia 2013
Storage	Researchers hacked into the smart battery controller and modified battery data [7]	US 2011

in a separate demonstration, they remotely controlled a Jeep Cherokee, cutting acceleration and disabling its brakes. *Smart buildings* have also been exploited: one breach, routed through heating, ventilation, and air conditioning (HVAC) systems at a major retailer, exposed roughly 40 million payment-card accounts; another demonstration achieved unauthorized access to the building management system of a large technology firm's office. These cases demonstrate how the impending scale and geographic dispersion of power-electronic assets may pose significant cyber-physical threats to modern grids.

1.2 Cyber and Physical Resilience

1.2.1 Importance

Resilience is commonly described as a system's capacity to foresee disruptions, withstand their effects, adapt, and restore function rapidly [8]. Beyond hazards driven by the physical environment (e.g., extreme weather), recent years have seen a surge in reported cyber incidents—rising by nearly 2000.

For physical disturbances to a power system (hurricanes, floods, sandstorms, etc.), enhancement strategies for physical resilience are often organized into

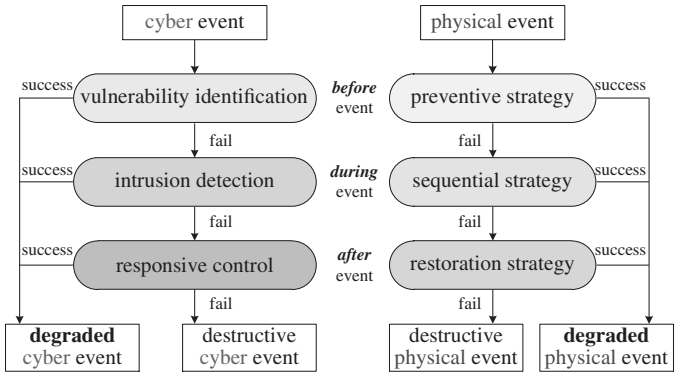

Figure 1.2 Cyber or physical resilience before, during, and after a cyber or physical event.

the three stages in Figure 1.2 [9]: (1) assessment and/or resource pre-allocation *before* the event; (2) sequential response and/or attack–defense interactions *during* the event; and (3) system restoration *after* the event. Analogously, cyber resilience measures for inverter-interfaced grids are typically grouped into three phases—*identification*, *detection*, and *response*—an approach widely adopted by industry [2, 10] and academia [9, 11].

As depicted in Figure 1.2 [9, 10], *before* a cyber incident, defenders prioritize threat discovery, attack-path identification, and impact evaluation. *During* an incident, the focus shifts to timely detection using model-based or data-driven techniques. Both identification and detection aim to decouple cyber actions from physical consequences. *After* an incident, the objective is effective response and mitigation through cyber-resilient strategies.

In line with this, Table 1.2 gathers several cybersecurity regulations and roadmaps spanning critical infrastructure, industrial control, electric power systems, and power-electronic devices. At the critical-infrastructure level, we have the National Institute of Standards and Technology (NIST) Cybersecurity Framework and North American Electric Reliability Council (NERC) Cyber Instruction Guide. For industrial control systems, foundational documents include International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27000, IEC TS 62443, and the NERC Critical Infrastructure Protection (CIP) standards. The power-system layer integrates federal guidance and technical standards—NIST Technical Note 2182, Institute of Electrical and Electronics Engineers (IEEE) 1547-2018, IEEE C37.240, NIST Interagency Report (NISTIR) 7628, and IEC TS 62351. The power-electronics category highlights IEEE 1686-2013 as a device-level security baseline.

Table 1.2 Cybersecurity regulation and roadmap for power systems.

Category	Regulation and roadmap	Institution	Time	Refs.
Critical infrastructure	Cybersecurity Framework	NIST	2018	[12]
	Cyber Instruction Guide	NERC	2018	[13]
Industrial control system	ISO/IEC 27000	ISO/IEC	2018	[14]
	IEC TS 62443	IEC	2007	[15]
	NERC CIP	NERC	2005	[16]
Power system	NIST Technical Note 2182	NIST	2021	[17]
	IEEE 1547-2018	IEEE	2018	[18]
	IEEE C37.240	IEEE	2015	[19]
	NISTIR 7628	NISTIR	2014	[20]
	IEC TS 62351	IEC	2007	[21]
Power electronics	IEEE 1686-2013	IEEE	2013	[22]

Table 1.3 further lists device-specific guidelines and roadmaps. For *generation* assets, photovoltaic systems are covered by Sandia National Laboratories (SNL)' Roadmap for PV Cybersecurity and PV Cybersecurity Report, complemented by National Renewable Energy Laboratory (NREL) guidance on PV plant operations. Wind generation is supported by U.S. Department of Energy (DoE) series—Roadmap for Wind Cybersecurity, Cybersecurity for Distributed Wind, and Cyber Resilience for Wind Power—alongside IEC 61400-25-1. In *transmission*, HVDC systems are addressed by U.S. DoE guidance on cyber-resilient HVDC and a vendor-oriented document on cybersecurity for HVDC and Flexible AC Transmission Systems (FACTS). *Prosumption* assets feature two subdomains: EVs, governed by ISO / Society of Automotive Engineers (SAE) 21434, United Nations (UN) Regulation No. 155, and SAE J2931/1; and microgrids, aligned with IEC 61850, IEEE 2030.9-2019, and an SNL microgrid cybersecurity reference. Smart buildings draw on CLC/TC 205 and IEC 62443. Finally, energy storage systems are framed by IEEE 2030.2-2015, National Fire Protection Association (NFPA) 855, and NERC guidance for battery energy storage systems (ESS).

1.2.2 Challenge

For inverter-interfaced power grids, cyber-physical resilience poses intrinsically interdisciplinary challenges. As illustrated in Figure 1.3, the analysis spans three coupled layers:

1. The *power system*, whose security and stability depend on the collective behavior of embedded power-electronic devices.

Table 1.3 Cybersecurity regulation and roadmap for representative power electronics devices in power systems.

Category	Device	Regulation and roadmap	Institution
Generation Cybersecurity	PV	Roadmap for PV Cybersecurity [23]	SNL
		PV Cybersecurity Report [24]	SNL
		Cybersecurity in PV Plant Operation [1]	NREL
	Wind	Roadmap for Wind Cybersecurity [2]	DoE
		Cybersecurity for Distributed Wind [25]	DoE
		Cyber Resilience for Wind Power [26]	DoE
		IEC 61400-25-1:2017 [27]	IEC
Transmission Cybersecurity	HVDC	Cyber-Resilient HVDC [28]	DoE
		Cybersecurity for HVDC and FACTS [29]	Hitachi
Prosumption Cybersecurity	EV	ISO/SAE 2143 [30]	ISO/SAE
		UN Regulation No.155 [31]	UN
		SAE J2931/1 [32]	SAE
	Microgrid	IEC 61850 [33]	IEC
		IEEE 2030.9-2019 [34]	IEEE
		Microgrid Cybersecurity Reference [35]	SNL
	Smart building	CLC/TC 205 [36]	CLC
		IEC 62443 [37]	IEC
Storage Cybersecurity	Energy storage system	IEEE 2030.2-2015 [38]	IEEE
		NFPA 855 [39]	NFPA
		Battery ESS Guidance [40]	NERC

2. The *power-electronic* devices, which provide superior controllability and observability but rely on metering/communication substrates that are exposed to cyber threats.
3. *Cyber-physical security*, which investigates data integrity (e.g., false-data injection and man-in-the-middle attacks), data availability (e.g., denial-of-service and time-delay attacks), and data confidentiality (e.g., malware, worms, and decryption). Together, these factors shape the resilience of the inverter-interfaced power grid.

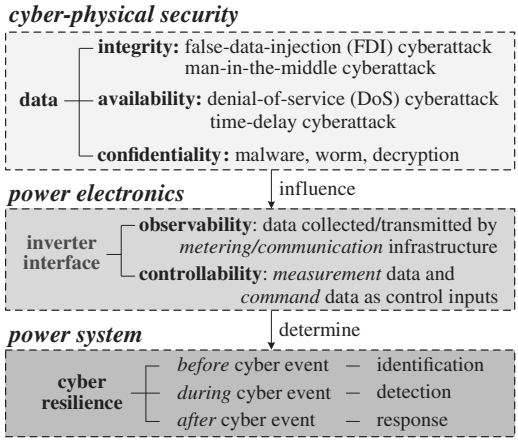

Figure 1.3 Interdisciplinary research fields for investigating the cyber-physical resilience of inverter-interfaced power grids.

Table 1.4 Similarities and differences of the cyber resilience between power electronics devices and power grids.

		Power grid operation	Power electronics control
Difference	Control loop	Open-loop control (measurement is independent of control output)	Closed-loop controller (measurement is feedback of control output)
	Timescale	Slow (minutes/hours)	Fast (milliseconds/seconds)
	Stealthiness	Achieved by satisfying the power flow equation	Achieved by corrective action of closed-loop controller
	Communication	Centralized architecture	Decentralized/distributed architecture
Similarity	Cyberattack	Data integrity/availability/confidentiality cyberattack on measurement/command data via metering/communication infrastructures	
	Cyberdefense	Identification/detection/response cyberdefense strategies before/during/after cyberattacks	

Specifically, as summarized in Table 1.4, the research challenges for cyber-physical resilience in inverter-interfaced power grids arise from two interlinked domains: the *power grid* and the *interconnected power electronics*. Their cybersecurity paradigms share commonalities yet also exhibit fundamental differences, each leading to distinct challenges.

Two similarities are salient. First, both device- and grid-level functions are vulnerable to attacks on measurement and control-command channels carried over metering/communication infrastructures via integrity (e.g., false data injection attacks), availability (e.g., denial-of-service attacks), and confidentiality (e.g., malware). Second, cyber resilience at both layers can be structured into three stages—before, during, and after an attack—through (1) identifying model and configuration vulnerabilities; (2) detecting malicious injections into measurement /command channels; and (3) responding to and mitigating attack-induced effects. These defense layers may be deployed independently or in coordination.
In addition, several differences require tailored treatments:

- *Control loop:* As shown in Figure 1.4, a key shift from grid-level to device-level cybersecurity is a move from an *open-loop* to a *closed-loop* paradigm. Grid applications such as optimal power flow (OPF) often operate effectively in an open loop, where measurements (e.g., real-time loads) are exogenous to dispatch decisions; attacks on these data can degrade economic efficiency [41], security [42], and stability [43]. By contrast, power-electronic controllers close the loop around measured quantities to track reference commands. When measurements and/or commands are compromised, corrective actions in voltage/current/power loops can drive devices into over-voltage, over-current, and thermal stress, endangering both the converter and the grid it supports.
- *Timescale:* The timescales of attack consequences differ markedly. In power grid OPF, attack-driven re-dispatch typically unfolds over minutes [41, 44]. For a converter's voltage controller, attack-induced excursions (e.g., over-voltage) can emerge within milliseconds [45]. The very fast control that damps small fluctuations and arrests large disturbances also leaves little time for detection, localization, and mitigation before damage becomes irreversible, highlighting a fundamental tension between fast feedback and attack tolerance.

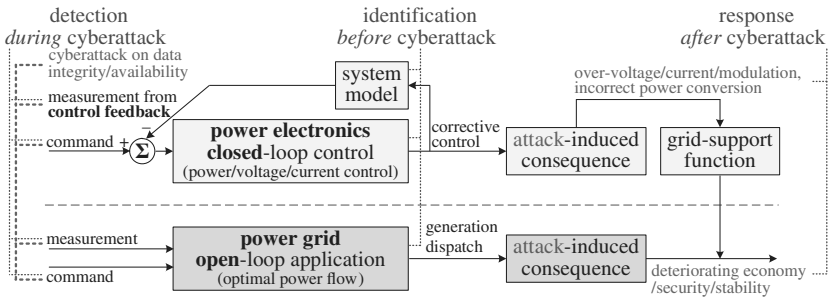

Figure 1.4 Comparison of the cyberattack/defense paradigms between power-electronics closed-loop control and power-system open-loop applications.

- *Stealthiness:* Stealth in grid-level attacks is often achieved by ensuring corrupted measurements satisfy power-flow relationships, thereby evading bad-data detection [46]. At the device level, stealthy attacks on local measurements can likewise appear stealthy to power-electronic controllers [45], because closed-loop regulation drives measured variables to match (possibly corrupted) setpoints.
- *Communication:* Dominant threat surfaces map into different communication architectures. Bulk systems are commonly orchestrated via centralized control centers communicating with geographically dispersed assets, making centralized channels prime targets. Many power-electronic devices, however, operate with decentralized (local measurements [47]) or distributed (peer-to-peer exchange [45]) schemes, shifting adversarial focus to local or distributed links.

Beyond cross-domain physical differences, research challenges also depend on research viewpoints—*cyberattacker*, *cyber defender*, and *system operator*:

- *Cyberattacker:* As the proverb goes, "*Forewarned is forearmed.*" That is, effective defense begins with understanding the adversary.
  - For inverter-interfaced power grids operating under hierarchical control with switching actions, what are the most critical vulnerabilities of such hybrid nonlinear dynamics? Do small, well-crafted attacks exist that precipitate severe consequences?
  - Moreover, grid operation must satisfy both security and economic efficiency; how should these metrics be jointly quantified? Where are the damage boundaries under worst-case attacks?
- *Cyber Defender:*
  - Temporally, attacks are rarely one-shot. Then, how can defenders respond sequentially and strategically to unfolding events?
  - Spatially, attacks may not be localized. Then, how can defenders coordinate cross-regional resources to build networked cyber immunity for interconnected subnetworks?
  - Economically, budgets are limited. Then, how can defenders quantify cyberdefense costs and benefits to allocate scarce resources against evolving, multi-vector attacks?
- *System Operator:*
  - Planning and operation act on different timescales yet are coupled. Then, how can preventive measures in planning shrink the attack-induced insecurity region? How can corrective actions in operation enlarge the cybersecurity margin with minimal disruption to routine practices?
  - With large-scale inverter integration, geometric characterizations of the physical security region can provide intuitive decision support. Then, how

can such regions be identified and expanded, and how can they be embedded into day-ahead and real-time workflows through inverter-security-constrained optimal power flow?
- At a system-wide level, as grids shift from synchronous-machine-based to inverter-interfaced architectures, how do cybersecurity paradigms differ across generation, transmission, prosumption, and storage stages?

1.3 Focus of This Book

The scope of this book is organized by three critical perspectives regarding the cyber-physical resilience of inverter-interfaced grids: the *cyberattacker*, the *cyber defender*, and the *system operator*.

- *Cyberattacker:*
  - Chapter 2: Investigate the cyberattack bifurcation hyperplanes of both voltage-source converter HVDC and current-source converter HVDC systems, revealing infinitesimal-attack-high-impact phenomena.
  - Chapter 3: Develop a stealthy false-data-injection attack tailored to small-signal angle stability (SSAS) with two coupled goals—primarily shrinking the SSAS margin while secondarily increasing operating cost.
- *Cyber Defender:*
  - Chapter 4: Develop a two-timescale model of multi-infeed HVDC systems and their interconnected asynchronous AC grids to explicitly quantify attack-induced frequency deviations, capturing fast DC power-control dynamics and slower equivalent synchronous-generator dynamics.
  - Chapter 5: Propose a cyber-immune framework for power subnetworks that formalizes innate immunity and constructs acquired immunity against stealthy false data injection attacks.
  - Chapter 6: Present a cost-benefit defense methodology grounded in a spatiotemporal dual-attack evaluation model for hybrid AC/DC systems.
- *System Operator:*
  - Chapter 7: Design a cost-efficient two-stage defense that first contracts the stealthy attack-induced insecurity region and then—if residual risk remains—enlarges the cybersecurity margin.
  - Chapter 8: Develop a geometric framework to identify and systematically enlarge the security region for single-inverter systems, and establish *inverter-security-constrained* optimal power flow in multi-inverter settings.
  - Chapter 9: Provide a systematic survey of power-electronic equipment across generation, transmission, and end-use stages, covering the before/during/after phases of cyber incidents.

1.4 Summary

In summary, as a cyber-physical infrastructure, the inverter-interfaced power grid is highly exposed to cyber risks. If compromised, interacting devices can severely degrade system performance—triggering load shedding, generator trips, or even widespread blackouts—with unacceptable economic and social repercussions. These realities underscore the urgency and importance of advancing the cyber-physical resilience of inverter-interfaced power systems.

Accordingly, this chapter has compiled representative cyber incidents and cybersecurity roadmaps for inverter-interfaced grids. Moreover, this chapter articulates cross-domain research challenges arising from the shared and divergent characteristics of power systems and power electronics. In addition, this chapter outlines problem formulations from the viewpoints of cyberattackers, cyber defenders, and system operators. Finally, this chapter clarifies the focus of this book by mapping each chapter to these challenges.

References

1 A. Walker, J. Desai, D. Saleem, and T. Gunda, "Cybersecurity in photovoltaic plant operations," tech. rep., 2021.
2 A. Sanghvi, B. Naughton, C. Glenn, J. Gentle, J. Johnson, J. Stoddard, J. White, N. Hilbert, S. Freeman, S. Hansen, and S. Sheng, "Roadmap for wind cybersecurity," tech. rep., 2020.
3 T. K. S. Lab, "Experimental security research of Tesla autopilot," 2019.
4 C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, no. S 91, 2015.
5 B. Krebs, "Target hackers broke in via HVAC company," Krebs on Security, 2014.
6 K. Zetter, "Researchers hack building control system at Google Australia office," 2013.
7 C. Miller, "Battery firmware hacking," *Black Hat USA*, pp. 3–4, 2011.
8 Cabinet Office, "Keeping the country running: natural hazards and infrastructure," tech. rep., 2011.
9 L. Xu, Q. Guo, Y. Sheng, S. Muyeen, and H. Sun, "On the resilience of modern power systems: a comprehensive review from the cyber-physical perspective," *Renewable and Sustainable Energy Reviews*, vol. 152, p. 111642, 2021.
10 J. T. Johnson, "Roadmap for PV cyber security," tech. rep., 2017.
11 W. Xu and F. Teng, "A deep learning based detection method for combined integrity-availability cyber attacks in power system," *arXiv*, 2020.
12 Cybersecurity, Critical Infrastructure, *Framework for Improving Critical Infrastructure Cybersecurity*, 2018.

13 N. R. Guideline, "Cyber intrusion guide for system operators," North American Electric Reliability Corporation (NERC), Atlanta, GA, USA, 2018.

14 B. Lewis, "ISO/IEC 27000—key international standard for information security revised," International Organization for Standardization, 2018.

15 "Industrial communication networks network and system security part 1-1: terminology, concepts and models, IEC," tech. rep., International Electrotechnical Commission, 2009.

16 G. A. Francia III and E. El-Sheikh, "NERC CIP standards: review, compliance, and training," in *Global Perspectives on Information Security Regulations: Compliance, Controls, and Assurance*, pp. 48–71, 2022.

17 A. Gopstein, N. Hastings, L. Feldman, R. Agarwal, and N. Bartol, "Distributed energy resource security: potential guidelines and research topics," 2021.

18 "IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," in *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003)*, pp. 1–138, 2018.

19 "IEEE standard cybersecurity requirements for substation automation, protection, and control systems," in *IEEE Std C37.240-2014*, pp. 1–38, 2015.

20 V. Y. Pillitteri and T. L. Brewer, "Guidelines for smart grid cybersecurity," 2014.

21 "Power systems management and associated information exchange, data and communications security," in *IEC International Standard*, vol. 62351, 2007.

22 "IEEE standard for intelligent electronic devices cyber security capabilities," in *IEEE Std 1686-2013 (Revision of IEEE Std 1686-2007)*, pp. 1–29, 2014.

23 J. Johnson, "Roadmap for photovoltaic cyber security," tech. rep., 2017.

24 J. T. Johnson, "PV cybersecurity final report," tech. rep., 2019.

25 M. J. Culler, J. P. Gentle, B. Smith, F. Cleaveland, and S. Morash, "Cybersecurity guide for distributed wind," 2021.

26 GE Research, "Cyber-physical resilience for wind power generation," tech. rep., 2020.

27 "Wind energy generation systems - part 25-1: communications for monitoring and control of wind power plants - overall description of principles and models," in *IEC 61400-25-1:2017,* pp. 1–73, 2017.

28 R. Nuqui, "Cyber attack resilient HVDC system (CARDS)," tech. rep., 2019.

29 Hitachi Energy, "Cyber security services HVDC and FACTS," tech. rep., 2021.

30 D. Ward, *Automotive Cybersecurity: An Introduction to ISO/SAE 21434*. SAE International, 2021.

31 "Uniform provisions concerning the approval of vehicles with regard to the emission of pollutants according to engine fuel requirements," in *UN ECE Regulation*, vol. 83, 2005.

32 R. M. Pratt and K. Gowri, "Electric vehicle communications standards testing and validation-phase ii: Sae j2931/1," tech. rep., Pacific Northwest National Lab.(PNNL), Richland, WA, 2013.

33 R. E. Mackiewicz, "Overview of IEC 61850 and benefits," in *2006 IEEE Power Engineering Society General Meeting*, 8 pp, IEEE, 2006.

34 "IEEE recommended practice for the planning and design of the microgrid," in *IEEE Std 2030.9-2019*, pp. 1–46, 2019.

35 J. E. Stamp, C. K. Veitch, J. M. Henry, D. H. Hart, and B. Richardson, "Microgrid cyber security reference architecture (v2)," tech. rep., Sandia National Lab.(SNL-NM), Albuquerque, NM, 2015.

36 J. Baumeister and G. Fuchs, "Interaction between home energy management and smart appliances," *Energy Efficiency in Domestic Appliances and Lighting (EEDAL'17),* p. 1023, 2017.

37 IEC, "Industrial communication networks-network and system security," 2008.

38 "IEEE guide for the interoperability of energy storage systems integrated with the electric power infrastructure," in *IEEE Std 2030.2-2015*, pp. 1–138, 2015.

39 J. Lamb and M. Paiss, "Safety codes and standards update (winter2019/2020)," 2020.

40 N. R. Guideline, *Performance, Modeling, and Simulations of BPs-connected Battery Energy Storage Systems and Hybrid Power Plants.* Atlanta, GA: North American Electric Reliability Corporation, 2021.

41 X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, 2014.

42 H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung, Y. Zhang, and C.-K. Wen, "Local cyber-physical attack for masking line outage and topology attack in smart grid," *IEEE Transactions on Smart Grid*, vol. 10, pp. 4577–4588, 2019.

43 J. Hou, J. Wang, Y. Song, W. Sun, and Y. Hou, "Small-signal angle stability-oriented false data injection cyber-attacks on power systems," *IEEE Transactions on Smart Grid*, vol. 14, no. 1, pp. 635–648, 2023.

44 A. Abur, *Power System State Estimation: Theory and Implementation.* Power Engineering; 24, New York: Marcel Dekker, 2004.

45 C. Burgos-Mellado, F. Donoso, T. Dragičević, R. Cárdenas-Dobson, P. Wheeler, J. Clare, and A. Watson, "Cyber-attacks in modular multilevel converters," *IEEE Transactions on Power Electronics*, vol. 37, no. 7, pp. 8488–8501, 2022.

46 Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–33, 2011.

47 B. Chen, S.-I. Yim, H. Kim, A. Kondabathini, and R. Nuqui, "Cybersecurity of wide area monitoring, protection, and control systems for HVDC applications," *IEEE Transactions on Power Systems*, vol. 36, no. 1, pp. 592–602, 2021.