
# Cybersecurity challenges in renewable-dominated power grids addressing vulnerabilities and resilience strategies

Cell Reports
Physical Science

CellPress
OPEN ACCESS

Perspective

# Cybersecurity challenges in renewable-dominated power grids addressing vulnerabilities and resilience strategies

Ahmed S. Musleh,[1] Guo Chen,[1,*] Boyu Liu,[1] Simone Fan,[1] Ahmed Al-Durra,[2] S.M. Muyeen,[3] Zhao Yang Dong,[4] Mir Nahidul Ambia,[5] Blazhe Gjorgiev,[6] Shengyu Tao,[7,*] and Huadong Mo[8,*]

[1]School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW 2052, Australia
[2]Advanced Power and Energy Centre, Khalifa University of Science and Technology, Abu Dhabi 00000, UAE
[3]Department of Electrical Engineering, College of Engineering, Qatar University, Doha 00000, Qatar
[4]Department of Electrical Engineering, City University of Hong Kong, Hong Kong, China
[5]Grid Connection Studies, Nordex Group, Melbourne, VIC 3000, Australia
[6]Department of Mechanical and Process Engineering, ETH Zürich, Zürich 8092, Switzerland
[7]Department of Electrical Engineering, Chalmers University of Technology, Gothenburg 41296, Sweden
[8]School of Systems and Computing, The University of New South Wales, Canberra, ACT 2600, Australia
*Correspondence: guo.chen@unsw.edu.au (G.C.), shengyu.tao@chalmers.se (S.T.), huadong.mo@unsw.edu.au (H.M.)
https://doi.org/10.1016/j.xcrp.2026.103261

## SUMMARY

The global transition to renewable-dominated power systems is reshaping grid operation while introducing new cybersecurity risks. As renewable technologies scale and rely on digital control and communication platforms, the cyberattack surface expands and exposes critical vulnerabilities. Here, we report an assessment of cybersecurity threats in renewable-dominated grids by examining representative attack scenarios, including false data injection into power control, denial of service on distributed energy resources and cloud platforms, inverter parameter manipulation, and GPS time synchronization spoofing. These threats are shown to compromise system stability, reliability, and resilience. We further evaluate current industrial practices, regulatory frameworks, and emerging standards in addressing these risks. We find that existing approaches remain insufficient for the complexity of renewable-dominated systems. We conclude by identifying the root causes of past failures and outlining research and policy directions to strengthen cyber resilience in future power systems.

## INTRODUCTION

The history of cyberattacks dates back to the early days of computer networks, escalating in the 1990s with incidents like the 1998 Solar Sunrise targeting the US military systems and exposing weaknesses in the national security systems.[1] As technology evolves, attacks grow in scale and sophistication. They have advanced from isolated digital pranks to strategic tools of espionage, sabotage, and warfare, increasingly threatening the critical infrastructure, such as energy systems, with global consequences.[2]

Cyberattacks on energy and power systems have evolved dramatically over the past two decades, posing significant risks to global infrastructure. From the early days of the Slammer worm attack on a nuclear plant in Ohio in 2003 to the sophisticated malware infiltrations of 2024, the energy sector has been under constant siege. These attacks have targeted critical systems, such as industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems, resulting in severe disruptions and substantial financial losses (Figure 1). Upon reviewing these attacks, two particularly alarming trends have been noted. The first is the increasing numbers and consequences of the attacks, and the second is the increasing frequency of cyberattacks targeting renewable energy systems.[3] As the world transitions to clean energy sources, cybercriminals have adapted their tactics to exploit vulnerabilities in these emerging technologies. Notable incidents include the 2019 denial-of-service attack on sPower's renewable generation, which disconnected over 500 MW from the grid,[3] and the 2020 malware attack on wind SCADA systems in Azerbaijan, allowing remote control and monitoring of wind turbines.[4] The impact of these attacks on renewable energy infrastructure is profound. In 2022, Germany faced two major incidents: Wiper malware on satellite communications resulted in the loss of monitoring for 5,800 wind turbines, and Conti ransomware disconnected 2,000 wind turbines from their control systems.[5] Moreover, many of the reported cyberattacks on energy and power systems targeted multiple entities simultaneously. For instance, during the 2023 Danish attack, weaknesses in firewalls enabled adversaries to remotely access energy infrastructure's ICS systems without authentication. Specialists characterized the incident as ''remarkable'' due to

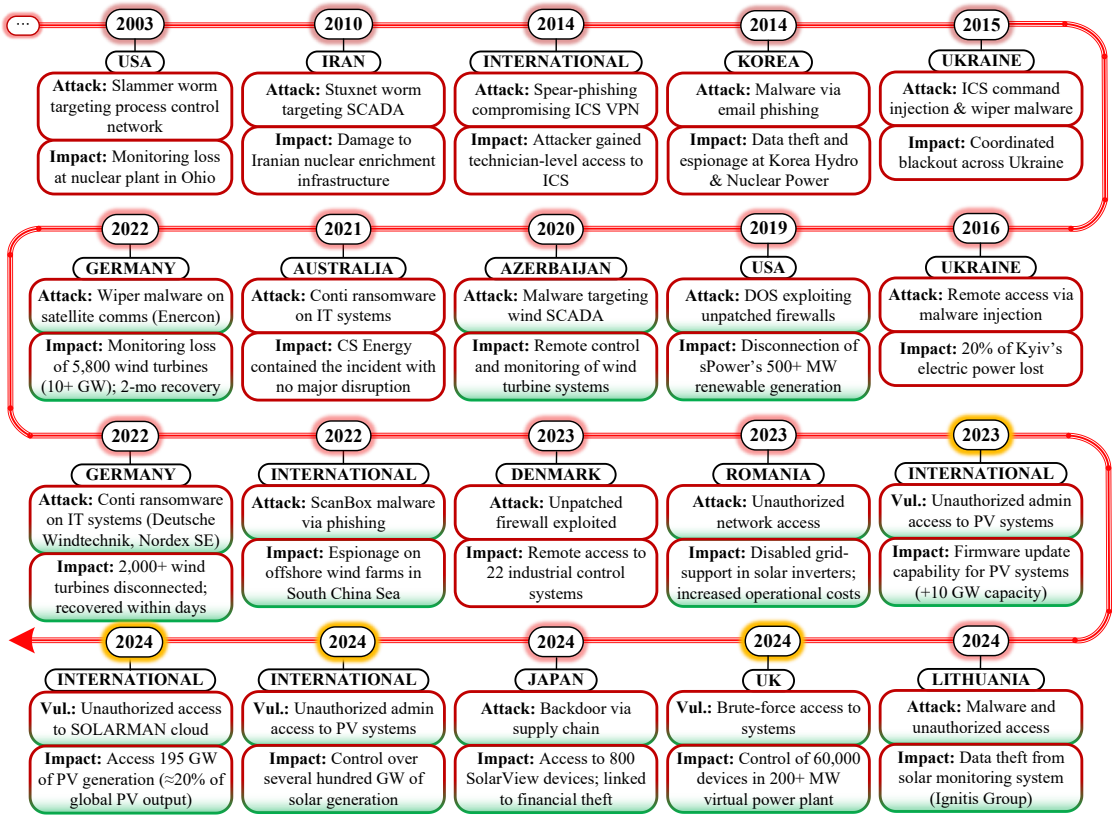


**Figure 1. Timeline of 20 selected major cyberattacks and vulnerabilities in energy and power systems (2003–2024)**

The 4 years highlighted in yellow indicate the detection of vulnerabilities (Vul.), where no actual attacks were implemented. The 12 incidents highlighted in green indicate that the attacks or vulnerabilities specifically targeted renewable energy systems. SCADA is supervisory control and data acquisition; ICS is industrial control systems; VPN is virtual private network; DOS is distributed denial of service; and malware is malicious software designed to harm, exploit, or compromise devices, networks, or data. Here, we only report major attacks targeting energy systems specifically.[3–15]

its precise harmonization. They emphasized that the attackers were able to pinpoint organizations with exposed devices and launch a synchronized campaign against them.[6] At the distribution level, a London-based security researcher in 2024 uncovered a critical cybersecurity vulnerability within a virtual power plant (VPP) system operated by the UK company GivEnergy. With these systems utilizing public networks, they present a real threat.

In this article, we analyze cybersecurity risks in renewable-dominated power systems through a structured examination of historical incidents, attack mechanisms, and system vulnerabilities. We present a curated timeline of attacks, develop a comparative taxonomy of threat vectors across conventional and renewable-rich systems, and establish mechanistic links between cyber intrusions and physical impacts such as voltage and frequency instability. We evaluate current standards and practices and identify persistent gaps and root causes. The results show that renewable-dominated grids introduce distinct and under-addressed cyber-physical risks, and we conclude that coordinated advancements in technology, policy, and operational practices are required to achieve resilient and secure future power systems.

## INCREASED CONTROLLABILITY AND CYBERSECURITY RISKS

Global renewable electricity generation is projected to exceed 17,000 TWh by 2030, an increase of nearly 90% from 2023. Several key milestones are expected over the next 5 years (Figure 2).[16] Already in 2025, electricity from renewables has overtaken coal-fired generation. By 2029, solar photovoltaic will likely surpass hydropower to become the largest renewable source.[16] In 2030, renewables are expected to supply 46% of global electricity, with wind and solar photovoltaic together accounting for 30%. This surge in renewable energy deployment is intrinsically linked to the rapid advancement of digital infrastructure and smart grid technologies, including information and communication technologies (ICT), transmission and distribution management systems, data centers, and advanced analytics platforms.[17] The integration of variable renewable sources, such as wind and solar, relies not only on these digital advancements but also on grid-enhancing technologies like flexible alternating current transmission systems (FACTS) and high voltage direct current (HVDC).[18] Furthermore, these renewable sources and other smart grid systems depend on smart inverters and

Please cite this article in press as: Musleh et al., Cybersecurity challenges in renewable-dominated power grids addressing vulnerabilities and resilience strategies, Cell Reports Physical Science (2026), https://doi.org/10.1016/j.xcrp.2026.103261





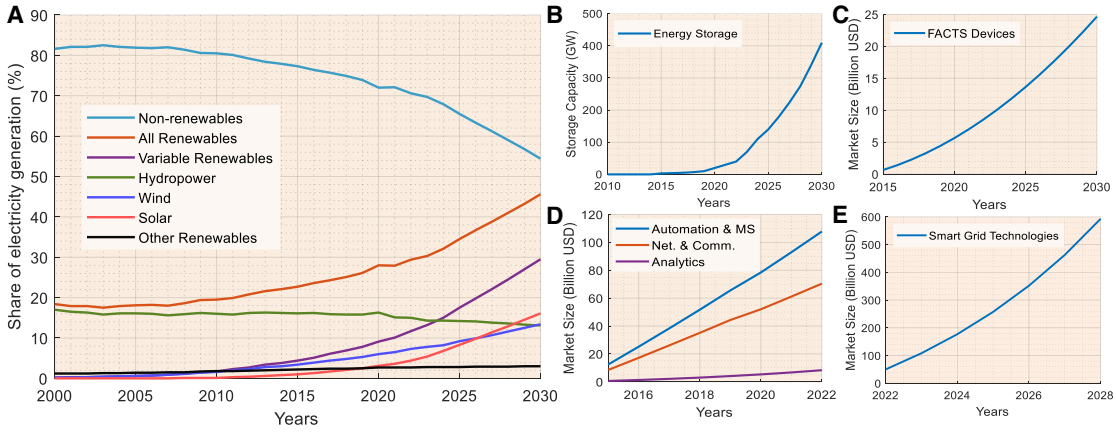


**Figure 2. Recent and forecasted trends in the energy and power systems industry**

(A) Share of renewable electricity generation by technology, 2000–2030.[16]

(B) Global cumulative energy storage installations, 2010–2030.[19]

(C) Global cumulative FACTS devices market size, 2015–2030.[20]

(D) Global cumulative investment in digital infrastructure in transmission and distribution electricity grids, 2015–2022.[21]

(E) Global cumulative market size in smart grid technology, 2022–2028.[17] The term smart grid covers various technologies, including advanced metering infrastructure (AMI), information and communication technologies (ICT), transmission and distribution management systems, data centers, analytics systems, and electricity supply security. The rapid expansion of smart grid and other grid-enhancing technologies, projected to exceed $600 billion by the 2030s, is closely tied to the growing share of variable renewable energy in electricity generation, which is expected to surpass 50% by the 2030s.

advanced control and communication mechanisms, often involving internet of things (IoT) devices, and different protocols to manage the power flow and security. These systems are typically connected to remote control centers. While this interconnectivity is essential for stable operation and efficient coordination, it also introduces new cyber and operational vulnerabilities into the power system.

Modern renewable energy systems operate within highly interconnected ecosystems involving many stakeholders, technologies, and ICT systems (Figure 3). These operations involve constant interaction with energy market operators, aggregators, retailers, technology providers, data centers, and cloud platforms. Real-time forecasting, dispatch, optimization, and control rely heavily on advanced digital infrastructure and communication networks.[22] Data centers and cloud services form the digital backbone of these systems, enabling scalable computation, storage, and integration across the electricity monitoring and control chain. Many independent players are involved, from hardware manufacturers to service operators. Clear governance rules and effective coordination mechanisms are essential to align all the physical and digital elements.[23] These operational rules are anchored in technical standards like IEC 61850 and IEEE 2030.5. Essentially, these standards guarantee that every device and system can communicate with one another reliably. This allows the electric grid to run automatically and in a distributed way.[24] Nonetheless, much of the communication of these entities employs public networks with questionable security measures.[25]

The many entities involved in renewable energy increase the vulnerabilities further. With the growing reliance on digital infrastructure, particularly cloud services and remote control software, the attack surface of energy systems has expanded. One notable example occurred in 2014, when a software vendor supplying virtual private network (VPN) tools to numerous energy companies in the US, Spain, France, and several other countries was attacked by Dragonfly attackers.[9] The attackers used VPN tools to reach and manage ICSs that run critical infrastructure like power plants, wind farms, and substations. They hid malicious code inside a legitimate software update, turning the VPN into a compromised version. Once installed on customer systems, the malware gave attackers the same access as authorized technicians. This allowed them to interact directly with control systems, letting them disrupt power flows or shut down operations entirely. This incident shows how a single weak point can ripple across international networks, highlighting the urgent need for strong cybersecurity and coordinated risk management in the renewable energy sector.

The growing penetration of variable renewable energy across power systems demands advanced monitoring and control capabilities. Wide-area monitoring and control systems are increasingly used to manage the stochastic nature of both utility-scale and distributed renewable generation. In Australia, Ausgrid's Project Edith enables dynamic pricing and allocation within distribution networks, allowing customer-owned energy resources to provide voltage support to the grid.[28] Similarly, Tesla has deployed large-scale virtual power plants using home solar systems and batteries that respond to electricity market signals in South Australia and California.[29] Distributed energy resources (DERs) now include smart functionalities, enabling them to react to external signals such as stability and price changes. These real-time control capabilities not only enhance grid flexibility but also increase the system's reliance on communication and digital networks that could introduce significant cybersecurity challenges with potentially global consequences.

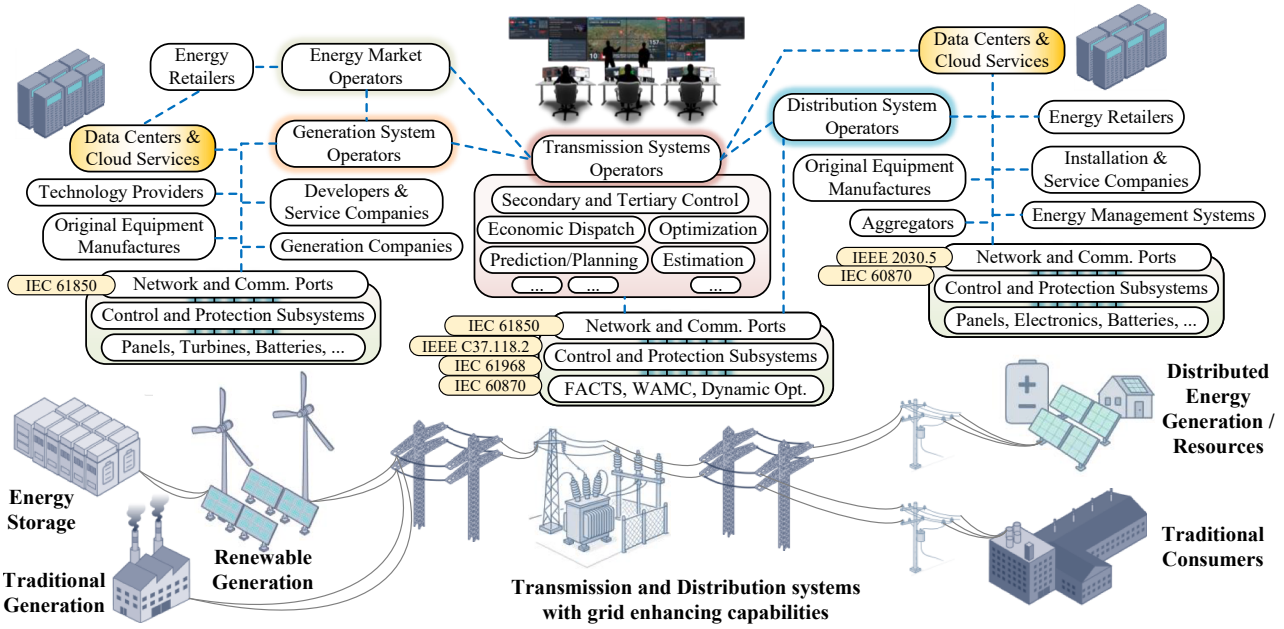


**Figure 3. Architecture of the major entities and systems involved in the operation of renewable energy systems in power grids**

The dashed blue lines resemble the communication and network links in different communication media and protocols. Some of these communication and networks have security measures, such as firewalls and VPN, at the system operators' control platform.[26] However, many of these systems use public internet for communication, especially at the DER systems or when communicating with third parties, such as the original equipment manufacturers.[25] The mentioned communication protocols are the main ones utilized in the industry; not all the protocols.[27]

## PLAUSIBLE CYBERATTACKS IN RENEWABLE-DOMINATED GRIDS

In traditional power grids, cyberattacks primarily target centralized control systems such as SCADA to gain unauthorized access, disrupt operations, and cause outages. However, in renewable-dominated grids, the attack surface expands significantly due to the new entities involved, the decentralized nature of DERs, VPPs, and aggregator platforms (Table 1). For instance, compromising SCADA systems now includes targeting microgrid controllers and DER management platforms, which are often less standardized and more vulnerable. False data injection attacks (FDIAs) become more potent as they can manipulate DERs like prosumer-owned solar systems, affecting grid stability and market operations.[30] Denial of service (DoS) attacks, once focused on central systems, now threaten a vast array of network-connected devices, such as smart inverters, making defense more complex.[31] Inverter and DER parameter manipulation, previously rare, is now a critical threat due to the widespread use of poorly secured devices. Market manipulation also evolves, with attackers exploiting dynamic pricing and flexible markets to mislead DER operations. Time synchronization attacks, such as GPS spoofing, pose new risks by desynchronizing thousands of GPS-reliant devices, which can lead to grid instability.[32]

Insider threats grow with the increased involvement of third-party service providers, while supply chain attacks target mass-produced DER hardware and software, often lacking robust security.[33] Finally, coordinated multi-point attacks using botnets can exploit millions of internet-connected DERs simultaneously, a feasible scenario in renewable-dominated grids.[34] Overall, the transition to renewable energy introduces a broader, more complex cyber threat landscape, requiring enhanced security measures tailored to the unique vulnerabilities of decentralized grid architecture. A basic block diagram of a typical renewable energy system can be composed of two converters, control layers, and communication interfaces with external entities such as original equipment manufacturers (OEMs) and aggregators (Figure 4A). These systems rely on network and communication interfaces to operate and provide various grid support functions.[35] However, the reliance on data exchange and remote control makes them vulnerable to various cyber threats.

The effect of a simple FDIA on the reactive power control can have a huge impact on the grid, depending on the grid's size and the renewable energy system's capacity.[25] When malicious data are injected to manipulate the reactive power control, either to absorb or supply excessively (Figure 4B), it causes voltage magnitudes to deviate outside the standard operating bounds of ±0.1 pu, shown as the green zone. The deviation is immediate and persistent, indicating that an attacker could destabilize the voltage profile of the grid. Depending on the attack's scale, this could cause either overvoltage or undervoltage, leading to equipment loss, which may cascade into blackouts.

A major consequence of high renewable utilization is the reduced system strength, which indicates how much the grid's voltage changes in response to a major disturbance.[36] With the domination of renewable energy resources that are typically

Please cite this article in press as: Musleh et al., Cybersecurity challenges in renewable-dominated power grids addressing vulnerabilities and resilience strategies, Cell Reports Physical Science (2026), https://doi.org/10.1016/j.xcrp.2026.103261





**Table 1. Comparative analysis of plausible cyber-physical attack types, purposes, and emerging challenges in traditional centralized power grids versus renewable-dominated grids**

| Attack type | Attack purpose in traditional grids | Additional attack purposes in renewable-dominated grids | Notes on renewables-specific challenges |
|---|---|---|---|
| SCADA/EMS system compromise (via malware and phishing) | • unauthorized control over grid operation<br>• overloads, faults, or blackouts by disrupting central control systems | • attack DMS, VPPs, and aggregator platforms managing DERs<br>• manipulate microgrid controllers to desynchronize local grids | DER control platforms are more varied and less standardized, increasing entry points and vulnerabilities |
| False data injection attacks (FDIA) | • mislead grid state estimation<br>• wrong operator decisions or automated control errors (e.g., incorrect power flow control) | • manipulate local demand or renewable generation forecasts<br>• influence market prices (e.g., fake PV output and false demand profiles)<br>• trigger grid instability by misleading inverter controllers | greater reliance on data from distributed and untrusted sources (e.g., prosumer-owned systems) makes FDIA attacks more feasible and damaging |
| Denial of service (DoS/DDoS) | • block communication with central control systems<br>• uncoordinated or unsafe grid operation | • disrupt IoT-based DER communications, cloud control platforms, or grid-edge devices (e.g., smart inverters and EV chargers)<br>• disable aggregation servers or VPP platforms | a vastly increased number of endpoints (DERs and EVs) makes DoS/DDoS defenses harder, and edge computing platforms are new vulnerable targets |
| Inverter/DER parameter manipulation (via malware or misconfiguration) | • rare, as inverters are limited in traditional grids | • change reactive power control, frequency settings, and ride-through capability of inverters to destabilize the grid (e.g., cause voltage flicker and harmonic injection)<br>• misuse EV chargers or storage inverters to create demand/generation imbalances | inverter control is a major new attack vector, especially through poorly secured or default-configured inverters and storage systems like in DERs |
| Grid market manipulation (via price/signal interference) | • manipulate market offers or bids to cause economic disruption or unfair advantage for certain operators | • inject false price signals to mislead DER operation (e.g., battery charge/discharge timings)<br>• exploit flexible markets by generating phantom loads or false flexibility offers | dynamic pricing, VPP, and demand-response schemes in renewable grids present new avenues for market-based manipulation |
| Time synchronization attacks (GPS spoofing) | • desynchronize phasor measurement units to disrupt state estimation or fault localization | • disrupt grid-forming inverter control or microgrid synchronization<br>• cause DERs to misalign with grid frequency, inducing instability | widespread dependence on GPS-synced inverters and microgrids introduces time sync vulnerability across thousands of DERs |
| Insider threats (malicious operators, contractors) | • sabotage central control actions<br>• disable protection systems | • insert malicious code into the inverter firmware<br>• manipulate settings in cloud DER platforms or aggregator services | an increased number of third-party service providers (installers and aggregators) in renewable grids heightens insider attack risk |
| Supply chain attacks (hardware/software compromise at source) | • backdoors in SCADA or networking equipment<br>• trojanized firmware in critical devices | • compromise mass-produced IoT-enabled DER devices (e.g., smart meters, inverters, and EVs)<br>• install vulnerabilities during DER manufacturing | lower-cost, mass-produced DER devices often lack rigorous supply chain security, making this a growing risk |

(*Continued on next page*)

**Table 1. *Continued***

| Attack type | Attack purpose in traditional grids | Additional attack purposes in renewable-dominated grids | Notes on renewables-specific challenges |
|---|---|---|---|
| Coordinated multi-point attacks (botnets and mass IoT exploitation) | • rare (fewer attackable points)<br>• focus on a few critical nodes | • exploit thousands/millions of DERs simultaneously (e.g., targeting DER systems) to cause synchronized grid instability or demand/generation spikes | highly feasible in renewables grids due to the sheer number of DERs with internet connectivity and weak security configurations |

It is highlighting the expanded attack surface, diverse threat vectors, and increased vulnerabilities introduced by the integration of distributed energy resources (DERs), distributed management systems (DMS), virtual power plants (VPP), electric vehicle (EV), energy management systems (EMS), and internet of things (IoT) devices.

integrated into the grid via electronics-based converters, the system's strength is significantly reduced due to the lack of rotational inertia. The impact of basic FDIA on active power control under different grid strengths may have different impacts (Figure 4C). When the same FDIA is applied to a strong system (represented in orange), the frequency remains relatively stable, showing some resilience. However, in a weak system (yellow curve), the same attack leads to considerable oscillations and a drop in frequency, potentially triggering under-frequency protection relays or even system collapse.

To enhance system strength and stability, grid-forming converters are rising in the industry[37]; however, these systems come with more vulnerability challenges. Targeting the synchronization function of grid-forming converters can have a major impact on the grid operations.[38] These attacks can disrupt the converter's ability to maintain grid stability by feeding erroneous phase reference signals. Synchronization attacks can cause extreme frequency oscillations, such as attack 1 (Figure 4D), spiking above 60.5 Hz and dipping below 59.5 Hz before, while attack 2 shows a more moderate but still disruptive deviation. Similarly, in Figure 4E, the voltage profile under synchronization attack 1 sharply drops below 0.8 pu, while attack 2 causes sustained oscillations. These deviations can damage grid infrastructure, disturb loads, or cause widespread disconnection of inverter-based resources.

If such cyberattacks were to be coordinated across many renewable systems or implemented on a large scale, the consequences could be catastrophic.[25] For instance, multiple FDIAs could collectively destabilize voltage across an entire region, while synchronization attacks on several grid-forming units could impair the grid's ability to maintain a stable reference frame. These large-scale attacks are possible via firmware update attacks or supply chain attacks.[33] The interconnected nature of power systems means that local instability can rapidly escalate into regional blackouts. Thus, it is imperative to ensure the secure operation of modern power systems.

## INDUSTRY STATUS QUO

The rapid global expansion of renewable energy systems is creating a widening gap between deployment rates and cybersecurity readiness. The cybersecurity frameworks governing these systems are often lagging behind, compromising the reliability, safety, and resilience of power infrastructure.

In response to emerging threats, several countries and regulatory bodies have begun implementing frameworks and standards to secure the different types of renewable energy systems. For example, the United States launched the "Cybersecurity Labeling Program for Smart Devices," which empowers consumers to make informed decisions when selecting DERs based on cybersecurity attributes.[39] Similarly, the UK Department of Energy Security and Net Zero has proposed mandatory minimum cybersecurity requirements for renewable assets, aiming to enhance baseline protections across the supply chain and life cycle of these technologies.[40] In the European Union, the EU Cybersecurity Act establishes a union-wide certification framework for ICT products, services, and processes.[41] This streamlines compliance for companies operating across member states and ensures a consistent security baseline. On a technical level, such certifications can cover firmware updates, data encryption, authentication protocols, and vulnerability reporting mechanisms, all of which are critical features for renewable energy security. Australia has taken a significant step by officially adopting the AS IEC 62443 series as national standards to protect operational technology (OT) in critical infrastructure, including energy systems.[42] This standard provides a structured approach to cybersecurity throughout the life cycle of the systems, emphasizing risk-based assessments, defense-in-depth strategies, and secure integration with IT systems. Despite these recent initiatives, significant delays and gaps remain noticeable. For instance, many standards, such as IEEE 1547, for DERs interconnection, have only recently incorporated cybersecurity considerations.[43] Australia's key DER interconnection standard AS/NZS 4777.2 lacks explicit cybersecurity provisions.[44] As renewable energy penetration grows, the absence of robust, enforceable, and technology-specific security guidelines poses a major risk, especially for large-scale and vastly varied renewable energy systems. These systems are often commissioned with functionality as a primary objective, with cybersecurity treated as an afterthought, if at all.

Recent cyber incidents targeting energy infrastructure have revealed that even with existing security measures, vulnerabilities still persist. Notably, many attacks exploited outdated standards or the absence of specific cybersecurity protocols, such as the 2003 Slammer worm and recent PV system breaches in 2023–2024 (Table 2). Standards, such as NIST SP 800-series, IEC 61850, and IEEE 1547, were only introduced or updated after attacks occurred. Human error remains a frequent root cause,

Please cite this article in press as: Musleh et al., Cybersecurity challenges in renewable-dominated power grids addressing vulnerabilities and resilience strategies, Cell Reports Physical Science (2026), https://doi.org/10.1016/j.xcrp.2026.103261





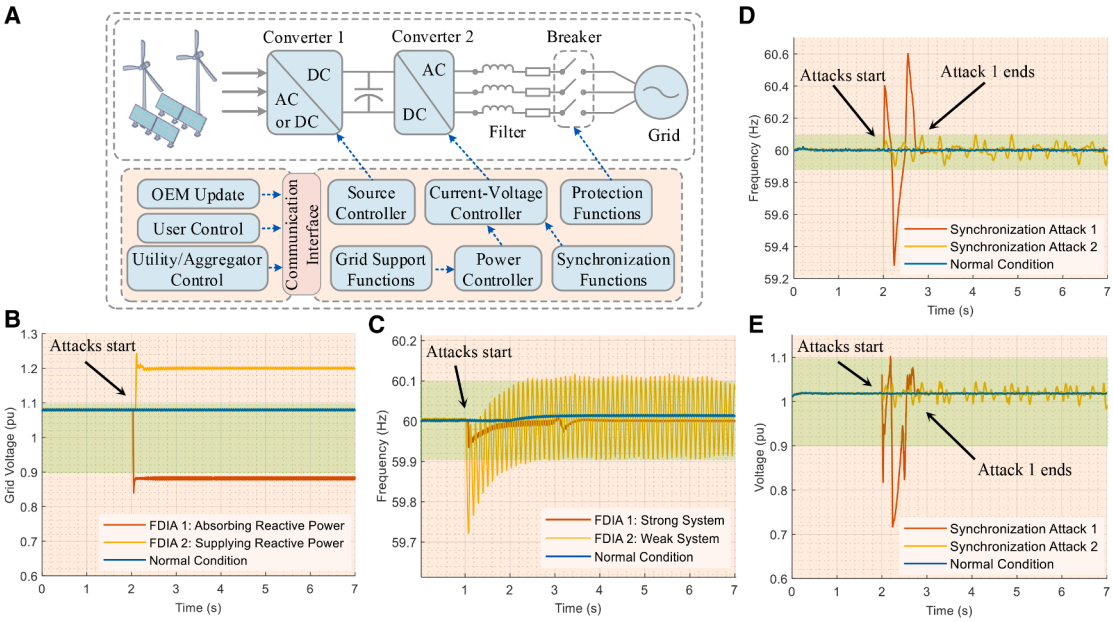


**Figure 4. Overview of cyberattacks' impacts on the operation and stability of renewable energy systems**

(A) Simplified block diagram of a typical renewable energy system with two converters and a control architecture.

(B) Impact of false data injection attack (FDIA) targeting reactive power output of renewable energy systems, resulting in a deviated voltage magnitude beyond the grid code specification ±0.1 pu (green region).

(C) Impact of FDIA targeting the active power output of renewable energy systems in strong and weak systems.

(D) Impact of synchronization attacks on grid-forming converter leading to varied frequency deviations.

(E) Impact of synchronization attacks on grid-forming converter leading to varied voltage magnitude deviations.

while patch management and secure authentication are ongoing challenges, especially in rapidly growing renewable sectors. Many attacks exploit known weaknesses or unpatched systems, raising questions about whether current regulatory efforts are sufficient or agile enough to keep pace with evolving threats and technologies. Ultimately, while global regulatory bodies have made progress, cybersecurity is still not deeply embedded into the development, deployment, and operation of renewable energy systems. A paradigm shift is needed where cybersecurity must be seen not as a compliance box, but as a foundational element of reliable, modern energy infrastructure.

## NEXT STEPS IN ENHANCING THE POWER SYSTEM RESILIENCE

Power system resilience will be a critical priority as grids absorb more renewable generation, distributed energy resources, IoT devices, and intelligent control systems. The scale of the cyber threat is massively increasing: more than 560,000 new malware variants appear every day and roughly four companies are compromised by cybercrime every minute.[46] In this setting, resilience must be built as a socio-technical capability that brings governments, industry, and researchers together to address people, processes, and technology at once. Responsibility is still fragmented, maintenance and updates are often deferred, and supply chains span borders with unclear ownership. To close these gaps, security standards must cover the full life cycle from design and integration through deployment and operation, rather than treating assets in isolation. Real incidents have shown how responsibility gaps between vendors, integrators, and operators lead to exploitable weaknesses, such as unpatched firewall paths. Treating breaches as crimes rather than technical mishaps strengthens accountability, improves cooperation with law enforcement, and discourages silence.

Resilience in practice means multi-layered protection at both network and device levels. Programs should fit how people actually work, align processes with security goals, and deploy tools that make the secure option the easiest action. Preventive cybersecurity practices are evolving toward application whitelisting, stronger cryptographic algorithms, stricter access controls, and network segmentation to prevent lateral movement. Mitigation should focus on securing communication interfaces, enforcing strong device authentication, and implementing real-time threat detection across all grid layers. Dynamically reconfigurable networks and secure firmware update mechanisms help systems adapt to threats in real time, while robust patch management frameworks limit impact and spread. The sector should move from reactive lists of risks to proactive models that include rigorous segmentation, precise maps of data flows into OT, and plans for controlled islanded operation to quarantine compromised assets. Rapid investigations and transparent disclosure are essential because delays expose peer organizations to repeat attacks.

Automation is central to narrowing the attacker's window. The time between the discovery of a vulnerability, release of a patch, and field deployment must shrink. Continuous scanning,

Please cite this article in press as: Musleh et al., Cybersecurity challenges in renewable-dominated power grids addressing vulnerabilities and resilience strategies, Cell Reports Physical Science (2026), https://doi.org/10.1016/j.xcrp.2026.103261



**Table 2. Analysis of selected recent reported attacks/vulnerabilities and related industrial standards and root causes**

| Attack | Year | Cybersecurity standards & year | Main root cause | More details |
|---|---|---|---|---|
| Slammer worm targeting the process control network at a nuclear plant[7] | 2003 | NERC CIP standards (2006); IEC 60870-5-101 (1995) | lack of protocols/standards | the Slammer worm entered the Davis-Besse nuclear plant through an unsecured contractor network, highlighting the need for robust cybersecurity protocols |
| Stuxnet targeting SCADA at nuclear infrastructure[8] | 2010 | ISA/IEC 62443 (2010); IEC 61850 (2005) | others (supply chain attack) | Stuxnet exploited multiple zero-day vulnerabilities to target Siemens PLCs, emphasizing the importance of securing supply chains |
| Spear-phishing targeting ICS VPN[9] | 2014 | NIST SP 800-53 Rev. 4 (2013); IEC 61850 (2005) | human factor | spear-phishing emails were used to gain unauthorized access to ICS VPNs, underscoring the need for user awareness training |
| Malware via email at Korea Hydro & Nuclear Power[10] | 2014 | KISA Guidelines (South Korea, 2013); IEC 60870-5-104 (2006) | human factor | North Korean group Kimsuky conducted a phishing attack, leaking sensitive data and highlighting insider threats |
| ICS command injection and Wiper malware at a power substation[11] | 2015 | NIST SP 800-82 Rev. 2 (2015); IEC 61850 (2005) | human factor | attackers used phishing to deploy malware, leading to power outages in Ukraine |
| Remote access via malware injection at a power substation[12] | 2016 | IEC 62351 (2007); NIST SP 800-82 Rev. 2 (2015) | human factor | the Crash Override malware targeted grid operations, exploiting remote access vulnerabilities |
| DoS exploiting unpatched firewalls[13] | 2019 | NIST SP 800-53 Rev. 5 (2020); IEC 61850 (2005) | unpatched/outdated systems | attackers exploited known vulnerabilities in unpatched firewalls, highlighting the importance of timely updates |
| Malware targeting wind SCADA[4] | 2020 | ISA/IEC 62443 (2018); IEC 61850 (2005) | unpatched/outdated systems | malware exploited outdated systems in wind SCADA operations, stressing the need for regular patch management |
| Conti ransomware on IT systems at CS Energy[14] | 2021 | ACSC Essential Eight (Australia, 2021); IEC 61850 (2005) | human factor | Conti ransomware was deployed through phishing emails, affecting CS Energy's IT systems |
| Wiper malware on satellite comms. of wind turbines[5] | 2022 | NIST SP 800-82 Rev. 2 (2015); IEC 61850 (2005) | others (supply chain attack) | Wiper malware targeted satellite communications, disrupting wind turbine operations |
| Conti ransomware on IT systems targeting wind generation systems[5] | 2022 | ACSC Essential Eight (Australia, 2021); IEC 61850 (2005) | human factor | similar to previous Conti attacks, phishing led to ransomware deployment in wind generation systems |
| ScanBox malware via phishing targeting wind farm operators[45] | 2022 | NIST SP 800-53 Rev. 5 (2020); IEC 61850 (2005) | human factor | phishing campaigns delivered ScanBox malware, compromising wind farm operator systems |
| An unpatched firewall was exploited, targeting ICS[6] | 2023 | NIST SP 800-82 Rev. 2 (2015); IEC 61850 (2005) | unpatched/outdated systems | attackers exploited unpatched firewalls to gain access to ICS, highlighting patch management deficiencies |

(*Continued on next page*)

Please cite this article in press as: Musleh et al., Cybersecurity challenges in renewable-dominated power grids addressing vulnerabilities and resilience strategies, Cell Reports Physical Science (2026), https://doi.org/10.1016/j.xcrp.2026.103261

**Table 2.** ***Continued***

| Attack | Year | Cybersecurity standards & year | Main root cause | More details |
|---|---|---|---|---|
| Unauthorized network access targeting solar inverters[3] | 2023 | NIST IR 8259 (2020); IEEE 1547 (2003) | lack of protocols/standards | weak authentication and exposed APIs allowed unauthorized access to solar inverters |
| Unauthorized admin access to PV systems[3] | 2023 | NIST IR 8259 (2020); IEEE 1547 (2003) | lack of protocols/standards | default credentials and the lack of security measures led to unauthorized admin access in PV systems |
| Malware and unauthorized access to solar monitoring systems[3] | 2024 | NIST SP 800-82 Rev. 2 (2015); IEEE 1547 (2003) | unpatched/outdated systems | malware exploited vulnerabilities in outdated solar monitoring systems, leading to unauthorized access |
| Brute-force access to DERs and VPPs[15] | 2024 | NIST SP 800-53 Rev. 5 (2020); IEEE 2030.5 (2018) | human factor | weak passwords allowed brute-force attacks on distributed energy resources and virtual power plants |
| Backdoor via the supply chain to SolarView devices[3] | 2024 | NIST SP 800-161 (2015); IEEE 1547 (2003) | others (supply chain attack) | a backdoor was introduced through the supply chain in SolarView devices, compromising security |
| Unauthorized admin access to PV systems[3] | 2024 | NIST IR 8259 (2020); IEEE 1547 (2003) | lack of protocols/standards | continued issues with default credentials led to repeated unauthorized access incidents |
| Unauthorized access to SOLARMAN cloud[3] | 2024 | NIST SP 800-53 Rev. 5 (2020); IEEE 2030.5 (2018) | lack of protocols/standards | weak cloud security measures allowed unauthorized access to SOLARMAN cloud services |

Note that many cyberattacks result from multiple vulnerabilities and root causes; however, only the main root cause is listed here.[3–15]

AI-assisted anomaly detection, and staged, orchestrated patching can accelerate the defensive cycle while keeping systems available. Emerging technologies can help: adversarial-aware AI for detection and response, blockchain for integrity of update chains and logs, edge computing for local autonomy, and quantum computing for next-generation cryptography. At the same time, quantum introduces risk, since future advances may render current encryption obsolete even as quantum-resistant methods promise stronger protection. Generative AI will accelerate both sides. Attackers will develop exploits faster, craft convincing spear-phishing, automate credential stuffing against OEM and virtual power plant portals, and generate synthetic telemetry that hides malicious activity. Defenders can respond with AI-assisted log triage, large-language-model code scanning for firmware and API gateways, content-filtered control channels that block out-of-policy set points, and red-team simulators that pair attack generation with converter dynamics to stress-test cyber-to-physics pathways before deployment. These capabilities should become part of acceptance testing and regular drills.

Despite ongoing programs, several gaps persist. Firmware update and supply chain assurance for mass-market distributed energy resources and inverters are inconsistent. Some vendors enforce signed updates, provide software bills of materials, and support remote attestation, while others do not. Incidents from 2023 to 2024 show repeat failures in update channels and third-party components. Operational dependencies on public networks and cloud services at the grid edge, via OEM portals and aggregator application interfaces, are often weakly segmented and inconsistently authenticated, enabling lateral movement from information technology and cloud into operational technology; the third-party links and choke points are mapped in Figure 3. Security that accounts for system dynamics is also immature. In low-inertia grids that rely on grid-forming inverters, small cyber perturbations in timing or measurement can cascade into voltage and frequency excursions. The destabilization pathways demonstrated in Figures 4D and 4E show that control robustness must be validated under adversarial conditions, not only under random faults or noise.

These gaps suggest six specific research priorities. First, design adversarially robust grid-forming control that can synchronize without phase-locked loops, remains stable under bounded sensor corruption, and is validated in hardware-in-the-loop with swarms of devices. Second, build a vendor-agnostic secure update fabric for the entire DER fleet that combines SBOM transparency, mandatory code signing, canary rollouts, and cryptographic attestation before grid-support functions can be enabled. Third, implement zero-trust architectures for virtual power plants and aggregators with brokered control channels, hardware-rooted device identities, and policy as code to prevent cloud-to-OT pivoting; the risk interfaces in Figure 3 provide a concrete basis. Fourth, automate the path from vulnerability to patch using continuous scanning, SBOM diffing, and risk-weighted scheduling to minimize downtime while closing known exposures. Fifth, protect market integrity by detecting price and dispatch gaming by compromised devices and by applying robust optimization that anticipates adversarial behavior. Sixth, plan defenses with system strength in mind by co-designing security controls and dynamic reserves and by quantifying how incidents shift frequency and voltage margins in weak areas, extending the analyses in Figures 4C–4E.

Advances will involve trade-offs. Network segmentation and backup communication add cost and complexity. Frequent patching and firmware updates require downtime and can reduce availability. Quantum-resistant cryptographic hardware increases deployment costs. Islanded microgrid capabilities may require oversizing resources or leaving capacity underutilized. Such costs are particularly burdensome for smaller utilities and developing regions. Governments are already moving with labeling, certification, and adoption of industrial cybersecurity standards, including IEC 62,443 in Australia, yet risks remain where standards lag practice and where DER and cloud edges are weakly governed, as summarized in Table 2. The missing pieces are clear. The sector needs mandatory fleet-level update assurance with signing, rollback protection, and attestation; independent attestation at the interconnection; privacy-preserving telemetry sharing for cross-operator detection; and dynamics-aware security validation that proves stability under adversarial disturbances. Because attackers are global and often coordinated, stronger international cooperation and shared exercises are essential. The fastest path to near-term risk reduction is to focus first on update assurance, edge segmentation, and adversarially validated control, while aligning regulation, coordinating globally, and making carefully optimized investment decisions.

## CONCLUSION

Renewables are transforming power systems and with them the cyber risk surface. This Perspective shows that incidents are no longer isolated anomalies but repeatable patterns that exploit weak update channels, exposed cloud and edge links, and control dynamics in low-inertia grids. We connect concrete cyber actions such as false-data injection and time-synchronization spoofing to voltage and frequency excursions and map where current standards and practices lag reality. The path forward is actionable. Mandate fleet-level update assurance and independent device attestation at interconnection. Engineer zero-trust, segmented edges for VPPs and DERs. Automate the vulnerability-to-patch pipeline and validate grid-forming controls under adversarial scenarios, not just noise or faults. Use AI to accelerate defense while hardening it against synthetic deception. Finally, treat transparency and cross-operator telemetry sharing as core reliability services. If we align people, process, and technology around these steps, renewables-dominated grids can be both clean and cyber-resilient.

## ACKNOWLEDGMENTS

This work is supported by Australian Research Council under grants FT190100156 and DP230100801. This work was also supported by Khalifa University of Science and Technology (KUST), Abu Dhabi, UAE, under award CIRA-2021-063.

## AUTHOR CONTRIBUTIONS

A.S.M. and G.C. conceptualized, designed, reviewed, revised, and drafted the manuscript. B.L., S.F., S.M.M., B.G., S.T., and H.M. reviewed and discussed

the manuscript. G.C. and A.A.-D. acquired funding. Z.Y.D., M.N.A., and A.A.-D. reviewed the manuscript before submission.

## DECLARATION OF INTERESTS

The authors declare no competing interests.

## SUPPLEMENTAL INFORMATION

Supplemental information can be found online at https://doi.org/10.1016/j.xcrp.2026.103261.

## REFERENCES

1. Monahan, C. (2023). Solar Sunrise: After 25 Years Are We 25 Years Wiser. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2023-02-28/solar-sunrise-after-25-years-are-we-25-years-wiser.
2. Slakaityte, V., Surwillo, I., and Berling, T.V. (2023). A new cooperation agenda for European energy security. Nat. Energy *8*, 1051–1053. https://doi.org/10.1038/s41560-023-01322-8.
3. Johnson, J. (2024). Public History of Solar Energy Cyberattacks and Vulnerabilities. https://dersec.io/reports/DERSec_Solar_Vulnerability_Summary_11-15-24.pdf.
4. Mercer, W. (2020). PoetRAT: Python RAT uses COVID-19 lures to target Azerbaijan public and private sectors. https://blog.talosintelligence.com/poetrat-covid-19-lures/.
5. Egan, M. (2022). A Retrospective on 2022 Cyber Incidents in the Wind Energy Sector and Building Future Cyber Resilience (Boise State University). Master's thesis.
6. Riotta, C. (2023). Denmark hit with largest cyberattack on record. BankInfoSecurity Critical Infrastructure Security, https://www.bankinfosecurity.com/denmark-hit-largest-cyberattack-on-record-a-23584.
7. Control Engineering (2023). Throwback attack: The slammer worm hits Davis Besse nuclear plant. https://www.controleng.com/throwback-attack-the-slammer-worm-hits-davis-besse-nuclear-plant/.
8. Kushner, D. (2013). The real story of Stuxnet. IEEE Spectr. *50*, 48–53. https://doi.org/10.1109/MSPEC.2013.6471059.
9. Hesseldahl, A. (2014). Hackers infiltrated power grids in US Spain. Vox Technology, https://www.vox.com/2014/7/1/11628504/hackers-infiltrated-power-grids-in-us-spain.
10. Lee, S. (2014). Revisiting the 2014 Korea Hydro and Nuclear Power Hack Lessons Learned for South Korean Cybersecurity (38 North). https://www.38north.org/2024/03/revisiting-the-2014-korea-hydro-and-nuclear-power-hack-lessons-learned-for-south-korean-cybersecurity/.
11. America's Cyber Defense Agency (2021). Cyber-attack against Ukrainian critical infrastructure. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.
12. Cherepanov, A., and Lipovsky, R. (2017). Industroyer: Biggest threat to industrial control systems since Stuxnet. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.
13. Goud, N. (2019). Utah Wind and Solar Power Generation Hit by a Cyber Attack (Cybersecurity Insiders). https://www.cybersecurity-insiders.com/utah-wind-and-solar-power-generation-hit-by-a-cyber-attack/.
14. CS Energy (2021). CS Energy responds to cyber security incident. https://www.csenergy.com.au/news/cs-energy-responds-to-cyber-security-incident.
15. Goodin, D. (2024). 512-bit RSA key in home energy system gives control of virtual power plant. Ars Technica, https://arstechnica.com/security/2024/08/home-energy-system-gives-researcher-control-of-virtual-power-plant/.
16. International Energy Agency (2024). Renewables 2024. https://www.iea.org/reports/renewables-2024.
17. ReportLinker and Statista (2023). Smart grid technology market size worldwide. https://www.statista.com/statistics/1301566/global-smart-grid-market-value/.
18. Su, T., Zhao, J., Gomez-Exposito, A., Chen, Y., Terzija, V., and Gentle, J.P. (2025). Grid-enhancing technologies for clean energy systems. Nat. Rev. Clean Technol. *1*, 16–31. https://doi.org/10.1038/s44359-024-00001-5.
19. BloombergNEF (2022). Global energy storage market to grow 15-fold by 2030. https://about.bnef.com/blog/global-energy-storage-market-to-grow-15-fold-by-2030/.
20. Business Research Insights (2024). FACTS devices market report overview. https://www.businessresearchinsights.com/market-reports/facts-devices-market-112443.
21. International Energy Agency (2023). Investment in digital infrastructure in transmission and distribution electricity grids. https://www.iea.org/data-and-statistics/charts/investment-in-digital-infrastructure-in-transmission-and-distribution-electricity-grids-2015-2022.
22. Kuzmin, E., Vlasov, M., Strielkowski, W., Faminskaya, M., and Kharchenko, K. (2024). Digitalization of the energy sector in its transition towards renewable energy A role of ICT and human capital. Energy Strategy Rev. *53*, 101418. https://doi.org/10.1016/j.esr.2024.101418.
23. Zografopoulos, I., Srivastava, A., Konstantinou, C., Zhao, J., Abiri Jahromi, A., Chawla, A., Nguyen, B., Siqi, B., Li, C., Teng, F., et al. (2025). Cyber-physical interdependence for power system operation and control. IEEE Trans. Smart Grid *16*, 2554–2573. https://doi.org/10.1109/TSG.2025.3538012.
24. Muyeen, S.M., and Rahman, S. (2017). Communication Control and Security Challenges for the Smart Grid (Institution of Engineering and Technology).
25. Musleh, A.S., Ahmed, J., Ahmed, N., Xu, H., Chen, G., Kerr, S., and Jha, S. (2024). Experimental cybersecurity evaluation of distributed solar inverters Vulnerabilities and impacts on the Australian grid. IEEE Trans. Smart Grid *15*, 5139–5150. https://doi.org/10.1109/TSG.2024.3393439.
26. Bhaskar, N., Ahmed, J., Masood, R., Ahmed, N., Kerr, S., and Jha, S.K. (2024). A comprehensive threat modelling analysis for distributed energy resources. ACM Trans. Cyber-Phys. Syst. *8*, 1–32. https://doi.org/10.1145/3678260.
27. Musleh, A.S., Chen, G., Dong, Z.Y., Wang, C., and Chen, S. (2020). Vulnerabilities threats and impacts of false data injection attacks in smart grids: An overview. In Proc. Int. Conf. Smart Grids Energy Syst.. https://doi.org/10.1109/SGES51519.2020.00021.
28. Ausgrid (n.d.). Project Edith. https://www.ausgrid.com.au/About-Us/Future-Grid/Project-Edith.
29. ARENA (2023). Tesla virtual power plant. https://arena.gov.au/projects/tesla-virtual-power-plant/.
30. Aouf, S., Derhab, A., and Guerroumi, M. (2020). Survey of false data injection in smart power grid: Attacks, countermeasures, and challenges. J. Inf. Secur. Appl. *54*, 102518. https://doi.org/10.1016/j.jisa.2020.102518.
31. Liu, S., Liu, X.P., and Saddik, A.E. (2013). Denial-of-service attacks on load frequency control in smart grids. In IEEE PES Innovative Smart Grid Technologies Conf, pp. 1–6. https://doi.org/10.1109/ISGT.2013.6497846.
32. Zhang, H., Peng, S., Liu, L., Su, S., and Cao, Y. (2020). Review on GPS spoofing-based time synchronisation attack on power system. IET Gener. Transm. Distrib. *14*, 4301–4309. https://doi.org/10.1049/iet-gtd.2020.0253.
33. Chen, J., Yan, J., Kemmeugne, A., Kassouf, M., and Debbabi, M. (2025). Cybersecurity of distributed energy resource systems in the smart grid: A survey. Appl. Energy *383*, 125364. https://doi.org/10.1016/j.apenergy.2025.125364.
34. Feng, Y., Huang, R., Zhao, W., Yin, P., and Li, Y. (2025). A survey on coordinated attacks against cyber physical power systems Attack detection and defense methods. Electr. Power Syst. Res. *241*, 111286. https://doi.org/10.1016/j.epsr.2024.111286.

35. Khalid, M. (2024). Smart grids and renewable energy systems Perspectives and grid integration challenges. Energy Strategy Rev. *51*, 101299. https://doi.org/10.1016/j.esr.2024.101299.

36. Kundur, P.S., and Malik, O. (2022). Power System Stability and Control, 2nd ed. (McGraw-Hill).

37. Musca, R., Vasile, A., and Zizzo, G. (2022). Grid-forming converters: A critical review of pilot projects and demonstrators. Renew. Sustain. Energy Rev. *165*, 112551. https://doi.org/10.1016/j.rser.2022.112551.

38. Kandasamy, N.K. (2020). An investigation on feasibility and security for cyberattacks on generator synchronization process. IEEE Trans. Ind. Inform. *16*, 5825–5834. https://doi.org/10.1109/TII.2019.2957828.

39. National Institute of Standards and Technology (2022). Cybersecurity labeling for consumers Internet of Things devices and software. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0.

40. UK Government (2023). Delivering a smart and secure electricity system: The interoperability and cyber security of energy smart appliances and remote load control. https://www.gov.uk/government/consultations/delivering-a-smart-and-secure-electricity-system-the-interoperability-and-cyber-security-of-energy-smart-appliances-and-remote-load-control.

41. European Commission (2025). EU cybersecurity certification framework. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.

42. Standards Australia (2025). Standards Australia adopts world's foremost standard for operational technology. https://www.standards.org.au/news/standards-australia-adopts-worlds-foremost-standard-for-operational-technology.

43. IEEE Application Guide for IEEE Std 1547™-2018 (2024). IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces. In IEEE Std 1547.2-2023, pp. 1–291. https://doi.org/10.1109/IEEESTD.2024.10534228.

44. Standards Australia (2020). AS NZS 4777.2 2020. https://www.standards.org.au/standards-catalogue/standard-details?designation=as-nzs-4777-2-2020.

45. Raggi, M., and Scenarelli, S. (2022). Rising tide Chasing the currents of espionage in the South China Sea. Proofpoint. https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea.

46. Statista (2025). State of malware worldwide Statistics and facts. https://www.statista.com/topics/8338/malware/?srsltid=AfmBOooTeK71tL6zbfz6ajRs-m0or8ZdrkWYskiDSuwYL_gmIbzm2L2N#topicOverview.