IJEES

International Journal of Electrical Engineering and Sustainability (IJEES)

ISSN (online): 2959-9229

https://ijees.org/index.php/ijees/index

ISI 2023-2024: (0.557) Arab Impact Factor: 1.51 SJIF 2024 = 5.274

Volume 3 | Number 3 | July-September 2025 | Pages 31-47

Article

Cyber-Resilience Strategies for Smart Microgrids: Classification, Construction, Recent Trends, and Policy Framework

Mohamed Khaleel [1*], Ziyodulla Yusupov[2], Hala J. El-Khozondar[4,5], Abdulgader Alsharif[6]

[1,2] Department of Electrical and Electronics Engineering, Faculty of Engineering, Karabuk University, Karabuk, 78050, Turkiye

[3]Electrical Eng. and smart systems dept., Faculty of Eng, Islamic University of Gaza, Palestine

[4]Dept. of materials and London centre for nanotechnology, Imperial College, Exhibition Road, London SW7 2AZ, UK

[5]Department of Electrical and Electronic Engineering, College of Technical Sciences, Sabha, Sabha, Libya

[*]Corresponding author: **lykhaleel@yahoo.co.uk**

Received: July 01, 2025 Accepted: August 27, 2025 Published: September 04, 2025

Abstract: Smart microgrids, as critical enablers of sustainable and decentralized energy systems, are increasingly dependent on the integration of cyber–physical systems (CPS) that combine distributed generation, energy storage, and advanced communication networks. While this digitalization enhances operational efficiency and flexibility, it also exposes microgrids to sophisticated cyber threats capable of undermining reliability, stability, and security. This article provides a structured analysis of cyber-resilience strategies for smart microgrids, addressing six core dimensions. First, the nature of CPS in smart microgrids is examined alongside the operational and security challenges associated with their convergence. Second, cyber-attacks are systematically classified to capture their diversity and potential impact, followed by a discussion of their construction and exploitation pathways within microgrid environments. Third, the study reviews recent trends in resilience strategies, including zero-trust architectures, defense-in-depth, secure firmware lifecycles, AI-driven anomaly detection, and advanced networking solutions such as SDN and TSN. Building on these insights, a multi-dimensional agenda is proposed that integrates governance, security architectures, communication resilience, incident response, intelligence sharing, capacity building, cryptographic agility, and AI-based monitoring. Finally, a policy framework is developed to guide regulators, operators, and stakeholders in translating these strategies into actionable measures for enhancing resilience.

Keywords: Smart Microgrids, Cyber–Physical Systems, Cyber-Resilience Strategies, Cyber-Attack Classification and Construction, Artificial Intelligence and Anomaly Detection.

1. Introduction

The rapid evolution of smart grids, characterized by interconnected AC-DC microgrids and power electronics-intensive architectures, underscored the critical role of information and communication technologies (ICT) in ensuring secure, stable, and efficient operations [1-4]. These systems rely heavily on advanced power electronic converters to interface distributed generation (DG), energy storage systems (ESS), and dynamic loads as demonstrated in Figure 1.

As the cyber and physical layers of these grids are deeply integrated, the reliability of microgrid operations is contingent upon the integrity and timeliness of cyber-physical data exchanges [5-9]. Any disruption, such as latency or data corruption, can compromise grid stability, efficiency, and operational safety. In this regard, European Union (EU) has significantly intensified its commitment to clean energy, with projected investments nearing USD 390 billion by 2025 [10-15].

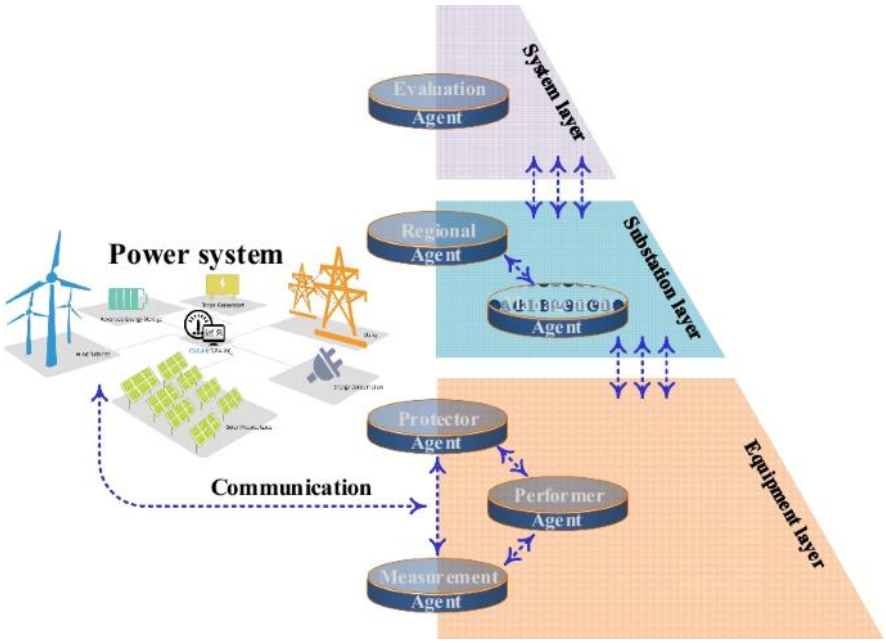

Figure 1. The fundamental network architecture of the DG microgrid system [16].

As smart grids become more vulnerable to cyber threats and cyber-attacks can have serious effects, a number of strategic initiatives have been started at the national and international levels to make grids more resilient. The United States and Canada have worked together to put the National Electric Grid Security and Resilience Action Plan into action. This plan is meant to improve the cybersecurity of new power infrastructures. The Department of Energy (DoE) has led a number of targeted cybersecurity research programs in the United States [17-20]. The Department of Energy (DoE) gave the University of Arkansas $12.2 million for the Secure Evolvable Energy Delivery Systems (SEEDS) project, which aims to create flexible cybersecurity solutions for energy delivery systems. The Department of Energy also gave the University of Illinois, Urbana-Champaign $28.1 million to start the Cyber Resilient Energy Delivery Consortium (CREDC) [21-25]. This group of experts from different fields works together to make critical energy systems more cyber resilient. Beyond North America, the European Union has also prioritized cybersecurity within its energy agenda, exemplified by the funding of the Smart Grid Protection Against Cyber-Attacks (SPARKS) project, aligned with the EU's 2030 energy security and digitalization objectives [26-30].

Smart microgrids that integrate renewable energy sources such as solar PV, wind, and hydrogen fuel cells offer enhanced sustainability, autonomy, and flexibility, but their increasing reliance on digitalized control and communication systems exposes them to diverse cyber threats [31-41]. To safeguard reliability, cyber-resilience strategies must combine preventive, adaptive, and recovery-oriented measures. These include governance frameworks and standards, secure multi-layered architectures, resilient communication protocols, AI-driven anomaly detection, and robust incident response mechanisms [42-46]. Moreover, resilience must address technology-specific vulnerabilities, such as inverter firmware in solar PV, pitch and yaw control in wind turbines, and hydrogen storage and monitoring systems in fuel cells. Policy support and capacity building, through cybersecurity audits, secure-by-design technologies, and specialized workforce training, are critical to ensuring resilience.

Distributed Flexible AC Transmission System (D-FACTS) devices, particularly Dynamic Voltage Restorers (DVR) and Distribution Static Compensators (D-STATCOM), play a crucial role in enhancing

voltage stability, reactive power balance, and power quality in renewable-rich smart microgrids [47-50]. However, their reliance on digital controllers and real-time communication exposes them to significant cyber vulnerabilities, including false data injection, denial-of-service, and unauthorized control manipulation. To address these risks, cyber-resilience strategies must combine governance and standards compliance, secure control architectures, resilient communication protocols, machine learning–based anomaly detection, and robust incident response mechanisms. Device-specific measures are also essential, such as protecting DVR synchronization algorithms and securing D-STATCOM reference signals [51-54]. Complementary policy frameworks should mandate cybersecurity testing, certification of updates, and operator training to strengthen system-wide defense. All in all, integrating cyber-resilience into D-FACTS deployment ensures that smart microgrids maintain stability and reliability while remaining capable of withstanding and recovering from cyber disruptions [55-61].

This article makes several key contributions to the growing body of knowledge on cyber-resilience in smart microgrids. First, it provides a comprehensive analysis of cyber–physical systems (CPS) within microgrid environments, identifying the operational and security challenges that arise from their convergence. Second, it develops a systematic classification and construction framework for cyber-attacks, offering deeper insights into how adversaries can exploit system interdependencies. Third, it synthesizes recent trends in resilience strategies, including zero-trust architectures, defense-in-depth models, secure firmware lifecycles, AI-based anomaly detection, and advanced networking techniques such as SDN and TSN. Fourth, it proposes a multi-dimensional agenda for cyber-resilience, which integrates governance, technical safeguards, communication reliability, incident response, collaborative intelligence sharing, capacity building, and cryptographic agility. Finally, it advances the field by formulating a policy framework that bridges technical measures with regulatory and institutional practices, thereby offering actionable guidance for policymakers, operators, and stakeholders. Collectively, these contributions provide both theoretical insights and practical tools for strengthening the resilience of smart microgrids against evolving cyber threats.

2. Cyber–Physical Systems in Smart Microgrids and Associated Challenges

This section explores the foundational concept of Cyber–Physical Systems (CPS) within the context of smart microgrids, emphasizing their multi-layered structure and the integration of physical power infrastructure with advanced information and communication technologies [62-68].

A. Concept of Cyber–Physical Systems

Smart microgrids are increasingly characterized by a high degree of power electronics integration, particularly for interfacing distributed generation (DG), energy storage systems (ESS), and a variety of dynamic loads. These systems exemplify the convergence of physical and cyber domains, where electrical infrastructure is intricately linked to and operated through advanced information and communication technologies (ICT). When integrating ICT with the physical power system, the CPS dynamic equation can be expressed as:

$$\dot{x}_{CPS}(t) = f_{phys}\big(x(t), u(t)\big) + f_{cyber}\big(c(t), d(t)\big) \quad (1)$$

Where, f_{phys} presents physical dynamics (power balance, grid equations). While, f_{cyber} demonstrates cyber-control functions (ICT commands, optimization, algorithms). $c(t)$ refers to communication signals (control signals, data flows). $d(t)$ depicts the cyber disturbances (latency, cyber-attacks, packet loss). As illustrated in Figure 2, a typical power electronics-intensive smart microgrid consists of a multi-layered cyber–physical system (CPS) architecture that facilitates coordinated operation, monitoring, and control.The cyber–physical model of a smart microgrid typically comprises four interdependent layers:

1) Physical Power System Layer

This foundational layer encompasses the core electrical components of the microgrid, including transformers, distributed energy resources (DERs), power electronic converters, circuit breakers, and end-user loads. These elements constitute the tangible infrastructure responsible for energy generation, conversion, and distribution.

2) Sensor and Actuator Layer

This layer serves as the interface between the physical and cyber domains. It includes a network of sensors and measurement devices that continuously monitor system states such as voltage levels, frequency, current flows, and breaker positions. The actuators, such as generator controllers, DER interfaces, and protection relays, execute the control commands derived from higher-level decision processes to maintain desired operational conditions.

3) Communication Layer

Serving as the data conduit, this layer facilitates real-time information exchange across the CPS architecture. It comprises hardware such as routers, switches, and communication media (wired or wireless), enabling seamless interaction between the sensor/actuator and control layers. The performance, reliability, and latency of this layer are critical to the stability and responsiveness of the entire microgrid.

4) Management and Control Layer

Positioned at the top of the CPS hierarchy, this layer functions as the intelligent control hub for the smart microgrid. It processes data acquired from the sensor layer, transmitted via the communication layer,and generates optimal control strategies for operational efficiency, reliability, and resilience. Control signals are then routed back through the communication layer to the actuators for execution. When cyber disturbances (e.g., delays, packet loss) are considered as following equation (2):

$$min_u\ J = \sum_{t=0}^{T} (\|x\ (t)\|_Q^2 + \|u\ (t)\|_R^2 + \lambda\ \tau(t)) \quad (2)$$

Where, the term min_u means minimize with respect to the control input. While, J is the objective (or cost) function being minimized. Q , R illustrates the weighting matrices for system states and control effort. τ(t) shows the communication delay penalty, λ displays resilience weight factor.

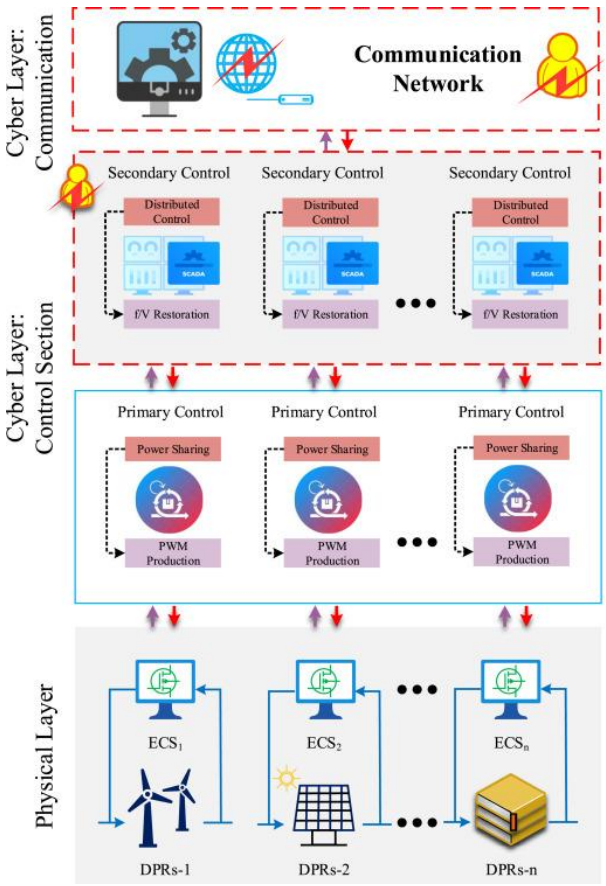

Figure 2. A typical power electronics-intensive smart microgrid consists of a multi-layered cyber–physical system (CPS) architecture [69].

3. Cybersecurity Standards and Protocols

To ensure the resilience and integrity of cyber–physical systems in smart microgrids, adherence to internationally recognized cybersecurity standards and protocols is essential. This section provides a critical investigation of several key frameworks and technical guidelines that inform best practices in securing smart microgrid infrastructures [70,74].

B. AMI System Security Requirements (AMI-SEC)

The Advanced Metering Infrastructure Security (AMI-SEC) initiative, developed under the UCA International Users Group (UCAIug), offers comprehensive security guidelines tailored to the AMI segment of the smart microgrid. AMI-SEC addresses the security needs of various AMI components, including communication networks, forecasting systems, meter management platforms, and home area networks. NERC Critical Infrastructure Protection (CIP)

The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) framework establishes mandatory cybersecurity standards for entities involved in operating the bulk electric system in North America. Comprising nine core standards and 45 specific requirements, the NERC CIP addresses issues such as identification of critical cyber assets, security management controls, personnel training, electronic and physical security perimeters, system security, incident response, and recovery planning.

C. NISTIR 7628

The NIST Interagency Report (NISTIR) 7628, developed by the National Institute of Standards and Technology (NIST), provides an extensive analytical framework for the development of robust cybersecurity strategies for smart grid environments. With over 600 pages across three volumes, this document offers utilities, electric vehicle infrastructure providers, and related stakeholders a structured methodology for addressing evolving threats in an increasingly interconnected grid landscape. The volumes cover (1) smart grid cybersecurity strategy, architecture, and high-level requirements; (2) privacy considerations; and (3) supporting analyses and references.

D. IEC 62351

The IEC 62351 standard, developed by the International Electrotechnical Commission (IEC), specifies security requirements for communication protocols used in power system operations, particularly those defined under the TC 57 series (e.g., IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970, and IEC 61968). It addresses key security objectives such as authentication using digital signatures, intrusion detection, prevention of eavesdropping, and protection against spoofing and replay attacks. The standard includes 16 parts, covering both protocol-level specifications and broader concerns like end-to-end security policies, access control, and key management.

E. ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC 27001 is the internationally recognized standard for information security management systems (ISMS), offering a comprehensive framework for evaluating and maintaining cybersecurity across diverse domains. It includes provisions for regular compliance checks, system security testing, and technical reviews to validate hardware and software security controls. ISO/IEC 27002 provides practical implementation guidance for ISO/IEC 27001, enhancing its applicability across various smart grid components and operational contexts.

F. GB/T 22239

The GB/T 22239 standard, developed in China, is titled Information Security Technology, Baseline for Classified Protection of Information System Security. It defines five levels of security protection capabilities for information systems, focusing on the ability to defend against, withstand, and recover from cyber threats. This standard can be applied to test and validate the compliance of all smart grid subsystems.

G. NIST SP 800-82

NIST Special Publication 800-82 provides detailed guidance on the security of Industrial Control Systems (ICS), which are integral to smart grid operations. Widely recognized and adopted internationally, this standard offers validated methodologies for implementing security controls, as well as recommendations for vulnerability assessments and penetration testing tools.

In essence, secure operation of smart microgrids, as highly interconnected cyber–physical systems, necessitates rigorous adherence to internationally recognized cybersecurity standards and protocols. As reviewed, frameworks such as AMI-SEC, NERC CIP, NISTIR 7628, IEC 62351, ISO/IEC 27001 and 27002, GB/T 22239, and NIST SP 800-82 provide comprehensive strategies for safeguarding critical infrastructure components across communication, control, and data management layers.

4. Classification of Cyber-Attacks

In smart microgrids, the Cyber-attacks plays a critical role in acquiring, transmitting, and processing data to govern the operation of the underlying physical infrastructure as illustrated in Figure 3. For the cyber-physical coordination to function effectively, data flow within the cyber system must be efficient, reliable, and timely. Disruptions to this data flow, whether by delay, corruption, or interception, can severely impair microgrid functionality. Cyber-attacks targeting smart microgrids can be broadly categorized into three types, based on the fundamental security principles they compromise: availability, integrity, and confidentiality [75-80].

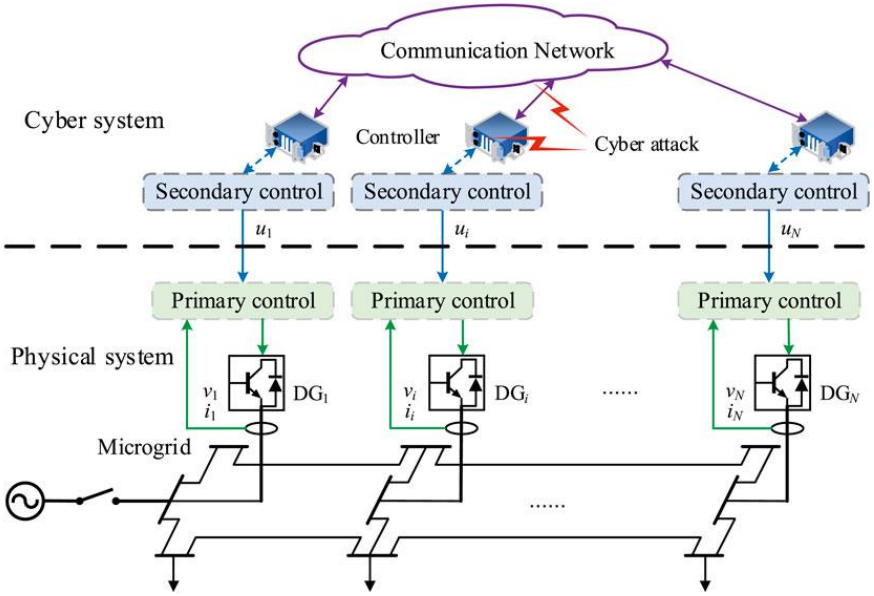

Figure 3. Disruption of blocks in microgrids within a cyber-attack [81].

H. Attacks on Data Availability

Ensuring data availability is paramount in smart microgrids, particularly for the real-time control of power electronic converters, especially under islanded conditions or during transient events. Attacks that primarily aim to obstruct or delay data transmission are classified as availability attacks. Notable examples include Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These can originate from a single node or multiple sources, typically by flooding the communication network with malformed or excessive data packets, thereby overwhelming routers, servers, or communication channels and rendering the system unresponsive.

I. Attacks on Data Integrity

Beyond availability, data integrity is essential to ensure that information remains accurate and unaltered throughout its lifecycle and under all operating conditions. Integrity attacks seek to manipulate or corrupt data, either measurements or control signals, within the communication network.

Such manipulations can lead to mis-operation of microgrid functionalities, including frequency and voltage regulation, power and energy management, islanding detection, and resynchronization. A prominent form of integrity attack is the False Data Injection (FDI) attack as displayed in Figure 4. FDI attacks represent one of the most insidious and technically sophisticated threats to smart microgrids. These attacks can be executed stealthily, modifying data in a way that does not alter the system's observability, thereby evading detection by system operators. For this reason, FDI attacks are often referred to as stealth attacks. Due to their severity and potential for widespread disruption, this paper devotes specific attention to the mechanisms, implications, and defense strategies against FDI attacks.

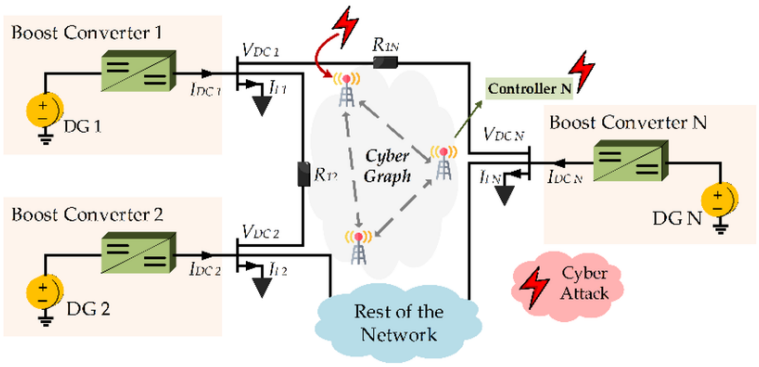

Figure 4. Cyber-physical model of a DC microgrid [82].

Figure 4 presents a cyber-physical model of a DC microgrid, highlighting the tight integration between the physical power infrastructure and the overlaid communication network. Each distributed generator (DG) is interfaced through a boost converter that regulates voltage and current contributions to the shared DC bus. These converters rely on real-time data exchange facilitated by a cyber-graph communication layer, which supports centralized or distributed control operations.

J. Attacks on Data Confidentiality

Data confidentiality pertains to protecting sensitive information from unauthorized access or exposure. Attacks targeting confidentiality involve eavesdropping on the communication network to extract private data, such as consumer identities, electricity usage patterns, and operational control strategies of the microgrid. While such breaches may not immediately compromise microgrid operation, the harvested data can serve as valuable intelligence for launching more damaging attacks, specifically those targeting data integrity and availability.

To summaries, the operation of smart microgrids is increasingly vulnerable to a diverse range of cyber-attacks that target the core tenets of data security: availability, integrity, and confidentiality. Among these, False Data Injection attacks pose particularly grave risks due to their subtlety and potential to cause large-scale disruption without triggering conventional alarms.

6. Construction of Cyber-Attacks

In recent years, considerable research efforts have been devoted to developing methodologies for constructing False Data Injection Attacks (FDIAs), particularly within cyber-physical systems such as smart microgrids. Typically, attackers possess partial knowledge of the cyber–physical architecture, although the availability of complete system information significantly enhances both the effectiveness and destructiveness of an attack. The degree of system knowledge and level of access attained by malicious actors are key determinants of the attack's severity and its potential to evade detection and mitigation mechanisms [83,84].

To evaluate how cyber-attacks can be constructed in power electronics-intensive smart microgrids, a review of the system's hierarchical control architecture is warranted. These microgrids commonly adopt a multi-layer control structure, comprising supervisory (outer layer) and primary (inner layer) control loops. The supervisory control center is responsible for collecting real-time data from distributed energy

resources (DERs), power electronic converters, and sensor networks, and issuing control decisions based on predefined operational objectives. These commands are transmitted to local controllers executing primary control functionalities. Typically, the supervisory layer is subdivided into tertiary control, which performs optimal power dispatch and regulates power exchange between the utility grid and the microgrid, and secondary control, which ensures frequency restoration, voltage balancing, and harmonic mitigation [85-87].

6. Recent Trends of Cyber-Resilience Strategies

Recent trends in cyber-resilience highlight a paradigm shift from reactive cybersecurity to proactive, intelligence-driven, and resilience-oriented approaches. Emerging practices such as zero-trust architectures, IEC 62443-based defense-in-depth, secure firmware lifecycles, AI-driven intrusion detection, and software-defined networking represent a growing emphasis on adaptability and layered protection. In addition, innovations in time-sensitive networking, resilience-oriented control co-design, automated islanding, and post-quantum cryptography readiness reveal the multidimensional nature of modern resilience efforts. Collectively, these developments underscore the need for an integrated strategy that aligns technical safeguards, operational practices, and policy frameworks to counter evolving cyber risks in smart microgrids as Table 1.

Table 1. Recent Trends of Cyber-Resilience Strategies for Smart Microgrids [88-93].

Trend	What it is	Techniques/ Standards	Use Cases	KPIs/Metrics
Zero-Trust Architectures for OT/ICS	Assume no implicit trust; verify every user/device/flow across microgrid networks.	Micro-segmentation, least-privilege, MFA, continuous verification; NIST SP 800-207.	Operator HMI access, vendor remote maintenance, DER gateway access control.	Unauthorized access rate, policy rule coverage, lateral movement attempts blocked.
IEC 62443-driven Defense-in-Depth	Layered security controls tailored to industrial automation and control systems.	IEC 62443-2/3/4 series, security zones & conduits, SL targets.	Segmenting inverter controls, protection relays, SCADA data paths.	Zone/conduit compliance, audit pass rate, patch compliance SLA.
Secure Firmware Lifecycle & SBOMs	Supply-chain transparency and secure updates for DER inverters, gateways, IEDs.	Secure boot, code signing, OTA with rollback, SBOM (SPDX/CycloneDX).	Inverter firmware updates, ESS controller patches.	Signed firmware coverage, mean patch latency, vulnerable component exposure time.
AI/ML Anomaly Detection (IDS)	Behavioral analytics over OT traffic and process signals to detect attacks/faults.	Unsupervised clustering, autoencoders, PCA, digital twins.	Detect spoofed measurements, false data injection, rogue DER behavior.	True/false positive rates mean time to detect (MTTD), coverage of assets/flows.
Software-Defined Networking (SDN) for OT	Centralized policy & flow control to enforce security and QoS deterministically.	OpenFlow, intent-based policies, ACL automation.	Prioritize protection relays, curtailment commands, PMU streams.	Policy enforcement success, path failover time, QoS jitter bounds.
Time-Sensitive Networking (TSN)	Deterministic Ethernet for bounded latency/jitter in control traffic.	IEEE 802.1Qbv/Qbu/AS, IEEE 1588 PTP.	Inverter sync, protection signaling, synchrophasor transport.	End-to-end latency, jitter, deadline-miss probability.

Resilience-Oriented Control Co-Design	Joint design of control and comms to tolerate delay/loss and cyber events.	MPC with delay penalties, event-triggered control, co-simulation (HIL).	Stable islanding, black-start, adaptive droop with comms delay.	Stability margins, recovery time, load served during incidents.
Automated Islanding & Black-Start Orchestration	Playbooks and automation to isolate, heal, and resynchronize.	Graph-based restoration, IEC 61850 GOOSE/SV, SOPs.	Cyber incident containment while keeping critical loads energized.	Islanding success rate, resynchronization time, critical load availability.
Threat Intelligence & Information Sharing	Collective defense via real-time intel feeds and sector ISACs.	STIX/TAXII, MISP, ATT&CK for ICS mapping.	Indicator blocking on gateways, rapid patch guidance.	Intel-to-action latency, coverage of TTPs, incident recurrence rate.
Cryptographic Agility & PQC Readiness	Ability to swap crypto suites; prepare for post-quantum algorithms.	TLS 1.3, ED25519, NIST PQC (KYBER/Dilithium) pilots, crypto-inventory.	DER onboarding, VPNs, firmware signing longevity.	Crypto-rotation time, PQC pilot coverage, deprecated cipher usage.

The evolution of cyber-resilience strategies for smart microgrids reflects an ongoing effort to strengthen the reliability, adaptability, and security of energy systems in the face of increasingly complex threats. Traditional perimeter-based defenses are no longer sufficient; instead, recent trends emphasize multilayered protections, real-time anomaly detection, secure supply chains, and coordinated recovery mechanisms.

7. Multi-Dimensional agenda of Cyber-Resilience Strategies

The evolution of smart microgrids has introduced a new paradigm where cyber and physical infrastructures are tightly interwoven to achieve efficiency, flexibility, and resilience. While this convergence enhances reliability and enables greater integration of renewable energy, it also expands the attack surface and exposes microgrids to sophisticated cyber threats. To address these challenges, a comprehensive understanding of cyber-resilience strategies is essential. A multi-dimensional perspective, encompassing governance, security architecture, communication resilience, incident response, intelligence sharing, human capacity building, cryptographic agility, and AI-driven detection, offers a structured framework for ensuring secure and sustainable operation. Table 2 provides an integrated view of these agendas, outlining their associated challenges and opportunities, advantages and disadvantages, and practical utilization within smart microgrid environments.

Table 2. Multi-Dimensional Agenda of Cyber-Resilience Strategies for Smart Microgrids.

Agenda	Challenges & Opportunities	Advantages	Disadvantages	Utilization
Defense-in-Depth Security Architecture	Challenge: Expanding attack surface from DER/ESS; Opportunity: Multi-layered security and segmentation.	Strong layered protection reduced lateral attack movement.	Complex to design and maintain; higher CAPEX/OPEX.	Applied in microgrid control centers and field devices (inverters, ESS controllers).
Resilient Communication Networks (SDN/TSN)	Challenge: Latency and jitter in real-time control; Opportunity: Deterministic and programmable networking.	Enables reliable control, prioritizes critical traffic.	Complexity of deployment; requires specialized equipment.	Used for SCADA, protection relays, PMU/synchrophasor communication.
Incident Response & Recovery Mechanisms	Challenge: Limited preparedness for ransomware/DoS; Opportunity: Automated islanding,	Reduces downtime, improves continuity of service.	Requires significant testing, may fail if not updated regularly.	Essential for emergency grid restoration and cyber incident containment.

	black-start orchestration.			
Threat Intelligence & Collaboration	Challenge: Limited cross-sector cooperation; Opportunity: Shared cyber threat intelligence platforms.	Improves early detection, strengthens collective defense.	Data privacy/legal issues; trust deficit between stakeholders.	Utilized by utilities, ISACs, regulators for real-time threat alerts.
Future-Proofing Cryptography (PQC Readiness)	Challenge: Quantum computing risks; Opportunity: Adoption of PQC and crypto-agility.	Ensures long-term data and system integrity.	Higher computational load; uncertainty about PQC standards.	Applied in VPNs, DER onboarding, firmware signing for microgrid devices.
AI/ML-driven Anomaly Detection	Challenge: False positives and explainability gaps; Opportunity: Advanced detection using digital twins and edge AI.	Detects novel attacks; scalable to large networks.	Can overwhelm operators with alerts; data privacy issues.	Real-time monitoring of DERs, ESS, and load behaviors.

The multi-dimensional view of cyber-resilience strategies highlights that no single measure can guarantee the security and reliability of smart microgrids. Instead, resilience requires a balanced approach that combines robust technical controls, effective governance, adaptive communication networks, and human capacity development. Each agenda presents distinct challenges, such as regulatory fragmentation, resource constraints, and emerging quantum threats, but also provides opportunities for innovation through standardization, intelligent automation, and advanced analytics. The advantages, ranging from improved continuity of service to long-term data integrity, must be weighed against disadvantages like cost, complexity, and operator burden.

8. Policy Framework

The complexity of cyber-resilience in smart microgrids calls for structured policy frameworks that can guide the development and implementation of effective strategies. These frameworks must address multiple layers of the ecosystem, including governance, technical defenses, incident management, collaboration mechanisms, and human capacity building. This study outlines five policy frameworks designed to strengthen cyber-resilience for smart microgrids as demonstrated in Figure 6.

Figure 6. Policy frameworks

A. Governance and Regulatory Alignment Framework

A governance and regulatory alignment framework are fundamental for enhancing cyber-resilience in smart microgrids. Establishing clear lines of authority, responsibility, and accountability among operators, regulators, and policymakers ensures that cybersecurity practices are not only well-defined but also enforceable. This framework emphasizes compliance with international standards such as ISO/IEC 27001, NIST Cybersecurity Framework, and IEC 62443, ensuring harmonization with global best practices.

B. Defense-in-Depth and Secure Architecture Framework

Equally important is the defense-in-depth and secure architecture framework, which focuses on building multilayered protection across smart microgrid infrastructures. This includes implementing network segmentation to separate operational technologies (OT) from information technologies (IT), thereby limiting the lateral spread of cyberattacks. Advanced measures such as strong authentication protocols, encryption of data exchanges, and intrusion detection systems (IDS) serve to fortify both digital and physical assets.

C. Incident Response and Continuity Framework

The incident response and continuity framework provide structured mechanisms for timely detection, containment, and recovery from cyber incidents. Smart microgrids, due to their distributed nature, require specialized Computer Security Incident Response Teams (CSIRTs) capable of rapidly mitigating threats while minimizing disruptions to power supply.

D. Collaboration and Information-Sharing Framework

A collaboration and information-sharing framework is also vital, as cyber-resilience in energy systems cannot be achieved in isolation. This framework encourages real-time exchange of cyber threat intelligence between utilities, equipment vendors, regulators, and government agencies through secure channels.

E. Capacity Building and Human-Centric Resilience Framework

Finally, a capacity building and human-centric resilience framework underscores the role of people and institutions in sustaining cyber-resilient smart microgrids. Continuous training programs for operators on cyber hygiene, digital forensics, and incident response are critical to minimizing human-related vulnerabilities.

The proposed policy frameworks collectively underscore the necessity of a holistic and multi-layered approach to strengthening cyber-resilience in smart microgrids. Governance and regulatory alignment provide the foundation for accountability and compliance, ensuring that operators and regulators adhere to internationally recognized standards. Defense-in-depth strategies create robust protective barriers that reduce vulnerabilities across physical and digital infrastructures. Incident response and continuity mechanisms enhance the ability to detect, contain, and recover from disruptions, while collaboration and information-sharing foster a culture of collective defense against evolving cyber threats. Finally, capacity building and human-centric measures emphasize the indispensable role of skilled personnel and institutional readiness in sustaining resilience. Together, these frameworks create a comprehensive pathway that balances technical safeguards, organizational preparedness, and cooperative engagement, enabling smart microgrids to operate securely, adapt to emerging threats, and maintain reliability as critical components of future energy systems.

9. Conclusion

This article has provided a comprehensive exploration of cyber-resilience strategies for smart microgrids, addressing their unique vulnerabilities and the evolving measures required to safeguard them. Beginning with an overview of cyber–physical systems (CPS) in smart microgrids, the analysis highlighted how the integration of distributed energy resources, storage systems, and advanced communication technologies creates both opportunities for efficiency and challenges in security. The classification of cyber-attacks clarified the diverse threat landscape, from denial-of-service and false data

injection to ransomware and supply chain compromises, while the construction of cyber-attacks in microgrid environments demonstrated how adversaries can exploit system interdependencies to disrupt stability and reliability.

The investigation of recent trends in cyber-resilience strategies underscored the paradigm shift from reactive security postures to proactive, resilience-driven approaches. Practices such as zero-trust architectures, IEC 62443-based defense-in-depth, secure firmware lifecycles, anomaly detection using AI/ML, and advanced communication solutions like SDN and TSN are emerging as critical enablers of robust resilience. Building upon these developments, the multi-dimensional agenda emphasized the necessity of aligning governance, security architectures, resilient communication, incident response, intelligence sharing, human capacity building, cryptographic agility, and AI-based anomaly detection within an integrated strategy. Finally, the policy framework provided a structured foundation for translating these strategies into actionable measures that can guide regulators, operators, and stakeholders toward coordinated and sustainable resilience.

Collectively, these discussions affirm that cyber-resilience in smart microgrids cannot be secured by isolated measures but requires a holistic and adaptive framework that integrates technical safeguards, human-centered initiatives, and policy alignment. While challenges such as regulatory fragmentation, resource constraints, and emerging quantum-era risks persist, opportunities exist to strengthen resilience through standardization, collaborative threat intelligence, and innovation in control and communication systems.

References

[1] Z. Ali *et al.*, "Cyber resilience in shipboard microgrids: adaptive hybrid artificial intelligent methods and systematic review," *Neural Comput. Appl.*, vol. 37, no. 22, pp. 17633–17674, 2025.

[2] A. D. Syrmakesis, C. Alcaraz, and N. D. Hatziargyriou, "Classifying resilience approaches for protecting smart grids against cyber threats," *Int. J. Inf. Secur.*, vol. 21, no. 5, pp. 1189–1210, 2022.

[3] D. K. Mishra, P. K. Ray, L. Li, J. Zhang, M. J. Hossain, and A. Mohanty, "Resilient control based frequency regulation scheme of isolated microgrids considering cyber attack and parameter uncertainties," *Appl. Energy*, vol. 306, no. 118054, p. 118054, 2022.

[4] M. Liu *et al.*, "Enhancing cyber-resiliency of DER-based smart grid: A survey," *IEEE Trans. Smart Grid*, vol. 15, no. 5, pp. 4998–5030, 2024.

[5] J. Dai, Z. Dai, and V. L. L. Thing, "Cyber-resilience enhancement with cross-domain software-defined network for cyber-physical microgrids against denial of service attacks," *Trans. Ind. Cyb-Phy. Sys.*, vol. 3, pp. 273–284, 2025.

[6] M. P. Korukonda, M. Shahidehpour, and L. Xie, "Cyber Resilience in Virtual Power Plants: A multiscale multilayer approach toward secure energy management," *IEEE Electrification Mag.*, vol. 13, no. 1, pp. 54–65, 2025.

[7] H. Shafei, L. Li, and R. P. Aguilera, "A comprehensive review on cyber-attack detection and control of microgrid systems," in *Power Systems*, Cham: Springer International Publishing, 2023, pp. 1–45.

[8] J. Ahmad *et al.*, "Cybersecurity in smart microgrids using blockchain-federated learning and quantum-safe approaches: A comprehensive review," *Appl. Energy*, vol. 393, no. 126118, p. 126118, 2025.

[9] M. Lezzi, A. Corallo, M. Lazoi, and A. Nimis, "Measuring cyber resilience in industrial IoT: a systematic literature review," *Manag. Rev. Q.*, 2025.

[10] A. S. Mohamed and D. Kundur, "Resilient cyber-physical system honeypots for cyberattacker engagement," *IEEE Trans. Industr. Inform.*, pp. 1–11, 2025.

[11] M. Hachimi, I. El Gaabouri, B. El Bhiri, S. Motahhir, and M. Boussetta, "Cybersecurity attacks and defense techniques in microgrid networks: A comprehensive survey," in *Lecture Notes in Networks and Systems*, Cham: Springer Nature Switzerland, 2025, pp. 182–199.

[12] O. Ali and O. A. Mohammed, "Experimental validation of a cyber-resilient frequency control for islanded microgrids," *IEEE Trans. Consum. Electron.*, pp. 1–1, 2025.

[13] F. Zargarzadeh-Esfahani, B. Fani, B. Keyvani-Boroujeni, I. Sadeghkhani, and M. Sajadieh, "Resilient oscillator-based cyberattack detection for distributed secondary control of inverter-interfaced Islanded microgrids," *Sci. Rep.*, vol. 15, no. 1, p. 20685, 2025.

[14] M. R. Habibi, J. M. Guerrero, and J. C. Vasquez, "Artificial intelligence for cybersecurity monitoring of cyber-physical power electronic converters: a DC/DC power converter case study," *Sci. Rep.*, vol. 14, no. 1, p. 22072, 2024.

[15] R. A. Mahmoud, O. P. Malik, and W. M. Fayek, "Smart technique for calculating fault current model parameters using short circuit current measurements," *Sci. Rep.*, vol. 15, no. 1, p. 29309, 2025.

[16] A. N. Sheta, G. M. Abdulsalam, B. E. Sedhom, and A. A. Eladl, "Comparative framework for AC-microgrid protection schemes: challenges, solutions, real applications, and future trends," *Prot. Control Mod. Power Syst.*, vol. 8, no. 1, 2023.

[17] M. R. Maghami, A. G. O. Mutambara, and C. Gomes, "Assessing cyber attack vulnerabilities of distributed generation in grid-connected systems," *Environ. Dev. Sustain.*, 2025.

[18] H. Naeem, F. Ullah, and G. Srivastava, "Classification of intrusion cyber-attacks in smart power grids using deep ensemble learning with metaheuristic-based optimization," *Expert Syst.*, vol. 42, no. 1, 2025.

[19] D. Abraham, S. H. Houmb, and L. Erdodi, "Cyber-attacks on energy infrastructure—A literature overview and perspectives on the current situation," *Appl. Sci. (Basel)*, vol. 15, no. 17, p. 9233, 2025.

[20] M. A. Alomari *et al.*, "Security of smart grid: Cybersecurity issues, potential cyberattacks, major incidents, and future directions," *Energies*, vol. 18, no. 1, p. 141, 2025.

[21] A. Gulraiz *et al.*, "WAMS Operations in modern power systems: A median expectation-based state estimation approach for grid resilience towards cyber attacks," *Int. J. Electr. Power Energy Syst.*, vol. 170, no. 110898, p. 110898, 2025.

[22] M. Swain, N. Tripathi, and K. Sethi, "Identifying communication sequence anomalies to detect DoS attacks against MQTT," *Comput. Secur.*, vol. 157, no. 104526, p. 104526, 2025.

[23] W. Kang, Q. Liu, P. Zhu, W. Zhao, X. Liu, and G. Hu, "Coordinated cyber-physical attacks based on different attack strategies for cascading failure analysis in smart grids," *Wirel. Netw.*, vol. 30, no. 5, pp. 3821–3836, 2024.

[24] P. Li *et al.*, "A defense planning model for a power system against coordinated cyber-physical attack," *Prot. Control Mod. Power Syst.*, vol. 9, no. 5, pp. 84–95, 2024.

[25] N. Tatipatri and S. L. Arun, "A comprehensive review on cyber-attacks in power systems: Impact analysis, detection, and cyber security," *IEEE Access*, vol. 12, pp. 18147–18167, 2024.

[26] A. Aljohani, M. AlMuhaini, H. V. Poor, and H. M. Binqadhi, "A deep learning-based cyber intrusion detection and mitigation system for smart grids," *IEEE Trans. Artif. Intell.*, vol. 5, no. 8, pp. 3902–3914, 2024.

[27] Q. Lu, Q. Gao, J. Li, X. Xie, W. Guo, and J. Wang, "Distributed cyber-physical intrusion detection using stacking learning for wide-area protection system," *Comput. Commun.*, vol. 215, pp. 91–102, 2024.

[28] J. Amissah, O. Abdel-Rahim, D.-E. A. Mansour, M. Bajaj, I. Zaitsev, and S. Abdelkader, "Developing a three stage coordinated approach to enhance efficiency and reliability of virtual power plants," *Sci. Rep.*, vol. 14, no. 1, p. 13105, 2024.

[29] H. R. Sayarshad, "Optimization of electric charging infrastructure: integrated model for routing and charging coordination with power-aware operations," *NPJ Sustain. Mobil. Transp.*, vol. 1, no. 1, pp. 1–24, 2024.

[30] T. Song and J. Teh, "Coordinated integration of wind energy in microgrids: A dual strategy approach leveraging dynamic thermal line rating and electric vehicle scheduling," *Sustain. Energy Grids Netw.*, vol. 38, no. 101299, p. 101299, 2024.

[31] S. Dawn *et al.*, "Integration of renewable energy in microgrids and smart grids in deregulated power systems: A comparative exploration," *Adv. Energy Sustain. Res.*, 2024.

[32] M. Khaleel *et al.*, "Battery technologies In electrical power Systems: Pioneering secure energy transitions," *J. Power Sources*, vol. 653, no. 237709, p. 237709, 2025.

[33] Y. F. Nassar *et al.*, "Design of reliable standalone utility-scale pumped hydroelectric storage powered by PV/Wind hybrid renewable system," *Energy Convers. Manag.*, vol. 322, no. 119173, p. 119173, 2024.

[34] M. Khaleel and M. Elbar, "Exploring the rapid growth of solar photovoltaics in the European Union," *Int. J. Electr. Eng. and Sustain.*, pp. 61–68, 2024.

[35] M. Khaleel, Z. Yusupov, and S. Rekik, "Exploring trends and predictions in renewable energy generation," *Energy 360*, vol. 4, no. 100030, p. 100030, 2025.

[36] Y. F. Nassar *et al.*, "Regression model for optimum solar collectors' tilt angles in Libya," in *2023 8th International Engineering Conference on Renewable Energy & Sustainability (ieCRES)*, 2023.

[37] Y. F. Nassar *et al.*, "Sensitivity of global solar irradiance to transposition models: Assessing risks associated with model discrepancies," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 11, no. 100887, p. 100887, 2025.

[38] Y. Nassar and M. Khaleel, "Sustainable development and the surge in electricity demand across emerging economies," *Int. J. Electr. Eng. and Sustain.*, pp. 51–60, 2024.

[39] M. Khaleel *et al.*, "Evolution of emissions: The role of clean energy in sustainable development," *Chall. Sustain.*, vol. 12, no. 2, pp. 122–135, 2024.

[40] M. Khaleel, Z. Yusupov, A. Ahmed, A. Alsharif, Y. Nassar, and H. El-Khozondar, "Towards sustainable renewable energy," *Appl. Sol. Energy*, vol. 59, no. 4, pp. 557–567, 2023.

[41] Y. F. Nassar *et al.*, "Carbon footprint and energy life cycle assessment of wind energy industry in Libya," *Energy Convers. Manag.*, vol. 300, no. 117846, p. 117846, 2024.

[42] P. Verma, T. Newe, G. D. O'Mahony, D. Brennan, and D. O'Shea, "Toward a unified understanding of cyber resilience: Concepts, strategies, and future directions," *IEEE Access*, vol. 13, pp. 49945–49965, 2025.

[43] G. Deffenbaugh and S. Kameneni, "Cyber resilience strategies throughout the system development lifecycle," in *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2025, pp. 504–509.

[44] S. M. Alhidaifi, M. R. Asghar, and I. S. Ansari, "Cyber resilience quantification: A probabilistic estimation model for IT infrastructure," *Reliab. Eng. Syst. Saf.*, vol. 265, no. 111473, p. 111473, 2026.

[45] A. Hajian, S. Rezaeinejad, K. Rayman, and S. Khorsandroo, "An innovative supply chain solution for information management in cyber resilience: Blockchain technology," *J. Innov. Knowl.*, vol. 10, no. 4, p. 100744, 2025.

[46] L. Tabansky and E. Lichterman, "PROGRESS: the sectoral approach to cyber resilience," *Int. J. Inf. Secur.*, vol. 24, no. 1, 2025.

[47] S. P. Agrawal *et al.*, "Exploring the effectiveness of adaptive randomized sine cosine algorithm in wind integrated scenario based power system optimization with FACTS devices," *Sci. Rep.*, vol. 15, no. 1, p. 7090, 2025.

[48] M. Tarafdar Hagh, M. A. Jabbary Borhany, K. Taghizad-Tavana, and M. Zare Oskouei, "A comprehensive review of flexible alternating current transmission system (FACTS): Topologies,applications, optimal placement, and innovative models," *Heliyon*, vol. 11, no. 1, p. e41001, 2025.

[49] M. F. Alwaeli, S. Galvani, and V. Talavat, "Addressing power quality challenges in hybrid renewable energy systems through STATCOM devices and advanced gray wolf optimization technique," *Results Eng.*, vol. 25, no. 104405, p. 104405, 2025.

[50] M. Khaleel *et al.*, "The impact of SMES integration on the power grid: Current topologies and nonlinear control strategies," in *New Technologies, Development and Application VII*, Cham: Springer Nature Switzerland, 2024, pp. 108–121.

[51] M. Khaleel, Z. Yusupov, M. Guneser, H. El-Khozondar, A. Ahmed, and A. A. Alsharif, "Towards hydrogen sector investments for achieving sustainable electricity generation," *jsesd*, vol. 13, no. 1, pp. 71–96, 2024.

[52] M. Khaleel, N. El-Naily, H. Alzargi, M. Amer, T. Ghandoori, and A. Abulifa, "Recent progress in synchronization approaches to mitigation voltage sag using HESS D-FACTS," in *2022 International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS)*, 2022.

[53] I. Imbayah, M. Hasan, H. El-Khozondare, M. Khaleel, A. Alsharif, and A. Ahmed, "Review paper on green hydrogen production, storage, and utilization techniques in Libya," *jsesd*, vol. 13, no. 1, pp. 1–21, 2024.

[54] M. Khaleel *et al.*, "An optimization approaches and control strategies of hydrogen fuel cell systems in EDG-integration based on DVR technology," *J. Eur. Syst. Autom.*, vol. 57, no. 2, pp. 551–565, 2024.

[55] M. Khaleel, Z. Yusupov, Y. Nassar, H. J. El-khozondar, A. Ahmed, and A. Alsharif, "Technical challenges and optimization of superconducting magnetic energy storage in electrical power systems," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 5, no. 100223, p. 100223, 2023.

[56] R. Gadal, A. Oukennou, F. El Mariami, A. Belfqih, and N. Agouzoul, "Voltage stability assessment and control using indices and FACTS: A comparative review," *J. Electr. Comput. Eng.*, vol. 2023, pp. 1–18, 2023.

[57] S. N. V. S. K. Chaitanya, R. A. Bakkiyaraj, B. V. Rao, and K. Jayanthi, "Optimal reactive power dispatch using modified-ant lion optimizer with flexible AC transmission systems devices," *Bull. Electr. Eng. Inform.*, vol. 14, no. 1, pp. 11–20, 2025.

[58] D. Sarathkumar, A. A. Stonier, and M. Srinivasan, "An extensive critique on FACTS controllers and its utilization in micro grid and smart grid power systems," in *Lecture Notes in Electrical Engineering*, Singapore: Springer Nature Singapore, 2023, pp. 323–333.

[59] "View of performance evaluation of MG systems interfaced with wind turbines employing DFIG technology," *Ijees.org*. [Online]. Available: https://ijees.org/index.php/ijees/article/view/82/44. [Accessed: 15-Sept-2025].

[60] J. Sarker, K. Sarker, S. K. Goswami, and D. Chatterjee, "Enhanced distribution system performance through optimal placement of hybrid dynamic voltage restorer," *Electr. Eng. (Berl., Print)*, vol. 107, no. 1, pp. 1059–1073, 2025.

[61] M. Khaleel, Z. Yusupov, M. Elmnifi, T. Elmenfy, Z. Rajab, and M. Elbar, "Assessing the financial impact and mitigation methods for voltage sag in power grid," *Int. J. Electr. Eng. and Sustain.*, pp. 10–26, 2023.

[62] S. Suprabhath Koduru, V. S. P. Machina, and S. Madichetty, "Cyber attacks in cyber-physical microgrid systems: A comprehensive review," *Energies*, vol. 16, no. 12, p. 4573, 2023.

[63] X. Bo *et al.*, "Modeling method for the coupling relations of microgrid cyber-physical systems driven by hybrid spatiotemporal events," *IEEE Access*, vol. 9, pp. 19619–19631, 2021.

[64] S. M. Khalil, H. Bahsi, H. O. Dola, T. Korõtko, K. McLaughlin, and V. Kotkas, "Threat modeling of cyber-physical systems - A case study of a microgrid system," *Comput. Secur.*, vol. 124, no. 102950, p. 102950, 2023.

[65] M. S. Abdelrahman, I. Kharchouf, H. M. Hussein, M. Esoofally, and O. A. Mohammed, "Enhancing cyber-physical resiliency of microgrid control under denial-of-service attack with digital twins," *Energies*, vol. 17, no. 16, p. 3927, 2024.

[66] Q. Wang, G. Zhang, and F. Wen, "A survey on policies, modelling and security of cyber-physical systems in smart grids," *Energy Convers. Econ.*, vol. 2, no. 4, pp. 197–211, 2021.

[67] M. Aslani, H. Hashemi-Dezaki, and A. Ketabi, "Reliability evaluation of smart microgrids considering cyber failures and disturbances under various cyber network topologies and distributed generation's scenarios," *Sustainability*, vol. 13, no. 10, p. 5695, 2021.

[68] Y. Wang, C.-F. Chen, P.-Y. Kong, H. Li, and Q. Wen, "A Cyber–Physical–Social Perspective on Future Smart Distribution Systems," *Proc. IEEE Inst. Electr. Electron. Eng.*, vol. 111, no. 7, pp. 694–724, 2023.

[69] I. Ahmed, A. M. El-Rifaie, F. Akhtar, H. Ahmad, Z. Alaas, and M. M. R. Ahmed, "Cybersecurity in microgrids: A review on advanced techniques and practical implementation of resilient energy systems," *Energy Strat. Rev.*, vol. 58, no. 101654, p. 101654, 2025.

[70] E. D. Ayele, J. F. Gonzalez, and W. B. Teeuw, "Enhancing cybersecurity in distributed microgrids: A review of communication protocols and standards," *Sensors (Basel)*, vol. 24, no. 3, 2024.

[71] C. V. Kifor and A. Popescu, "Automotive cybersecurity: A survey on frameworks, standards, and testing and monitoring technologies," *Sensors (Basel)*, vol. 24, no. 18, 2024.

[72] M. Muhammad, A. S. Alshra'a, and R. German, "Survey of cybersecurity in smart grids protocols and datasets," *Procedia Comput. Sci.*, vol. 241, pp. 365–372, 2024.

[73] S. Amanlou *et al.*, "Cybersecurity challenges in smart grid systems: Current and emerging attacks, opportunities, and recommendations," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 1965–1997, 2025.

[74] F. Harrou, B. Bouyeddou, A. Dairi, and Y. Sun, "Exploiting autoencoder-based anomaly detection to enhance cybersecurity in power grids," *Future Internet*, vol. 16, no. 6, p. 184, 2024.

[75] S. Yang, K.-W. Lao, H. Hui, J. Su, and S. Wang, "Secure frequency regulation in power system: A comprehensive defense strategy against FDI, DoS, and latency cyber-attacks," *Appl. Energy*, vol. 379, no. 124772, p. 124772, 2025.

[76] M. M. Alani, L. Mauri, and E. Damiani, "A two-stage cyber attack detection and classification system for smart grids," *Internet Things (Amst.)*, vol. 24, no. 100926, p. 100926, 2023.

[77] Y. Zhao, Y. Li, Y. Cao, and M. Yan, "Risk-based contingency analysis for power systems considering a combination of different types of cyber-attacks," *Appl. Energy*, vol. 348, no. 121551, p. 121551, 2023.

[78] S. H. Mohammed *et al.*, "Evaluation feature selection with using machine learning for cyber-attack detection in smart grid: Review," *IEEE Access*, pp. 1–1, 2024.

[79] A. Aflaki, M. Gitizadeh, R. Razavi-Far, V. Palade, and A. A. Ghasemi, "A hybrid framework for detecting and eliminating cyber-attacks in power grids," *Energies*, vol. 14, no. 18, p. 5823, 2021.

[80] H. Boyes and M. D. Higgins, "An overview of information and cyber security standards," *J. ICT Stand.*, pp. 95–134, 2024.

[81] G. Cao, R. Jia, and J. Dang, "Distributed resilient mitigation strategy for false data injection attack in cyber-physical microgrids," *Front. Energy Res.*, vol. 10, no. 845341, 2022.

[82] F. Nejabatkhah, Y. W. Li, H. Liang, and R. Reza Ahrabi, "Cyber-security of smart microgrids: A survey," *Energies*, vol. 14, no. 1, p. 27, 2020.

[83] O. T. Tambwe, C. O. Aigbavboa, O. I. Akinradewo, and P. A. Adekunle, "Measures to address cyber-attacks in construction project data management processes: A cybersecurity perspective," *IET Inf. Secur.*, vol. 2025, no. 1, 2025.

[84] R. Kateb, M. H. K. Tushar, C. Assi, and M. Debbabi, "Optimal tree construction model for cyber-attacks to wide area measurement systems," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 25–34, 2018.

[85] E. Naderi and A. Asrari, "Mitigating voltage violations in smart city microgrids under coordinated false data injection cyberattacks: Simulation and experimental insights," *Smart Cities*, vol. 8, no. 1, p. 20, 2025.

[86] M. Ghiasi, M. Dehghani, T. Niknam, A. Kavousi-Fard, P. Siano, and H. H. Alhelou, "Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform," *IEEE Access*, vol. 9, pp. 29429–29440, 2021.

[87] E. Yaghoubi, E. Yaghoubi, Z. Yusupov, and M. R. Maghami, "A real-time and online dynamic reconfiguration against cyber-attacks to enhance security and cost-efficiency in smart power microgrids using deep learning," *Technologies (Basel)*, vol. 12, no. 10, p. 197, 2024.

[88] V. Tzavara and S. Vassiliadis, "Tracing the evolution of cyber resilience: a historical and conceptual review," *Int. J. Inf. Secur.*, vol. 23, no. 3, pp. 1695–1719, 2024.

[89] S.-H. Choi, J. Youn, K. Kim, S. Lee, O.-J. Kwon, and D. Shin, "Cyber-resilience evaluation methods focusing on response time to cyber infringement," *Sustainability*, vol. 15, no. 18, p. 13404, 2023.

[90] G. Ahn, J. Jang, S. Choi, and D. Shin, "Research on improving cyber resilience by integrating the zero trust security model with the MITRE ATT&CK matrix," *IEEE Access*, vol. 12, pp. 89291–89309, 2024.

[91] J. Pavão, R. Bastardo, D. Carreira, and N. P. Rocha, "Cyber resilience, a survey of case studies," *Procedia Comput. Sci.*, vol. 219, pp. 312–318, 2023.

[92] J. Pavão, R. Bastardo, and N. P. Rocha, "Cyber resilience and healthcare information systems, a systematic review," *Procedia Comput. Sci.*, vol. 239, pp. 149–157, 2024.

[93] J. Stanik and J. Napiórkowski, "Cyber resilience as a new strategy to reduce the impact of cyber threats," in *Lecture Notes in Networks and Systems*, Cham: Springer Nature Switzerland, 2023, pp. 75–92.