Article

Not peer-reviewed version

Integrated Approaches for SG Management: Analysis, Vulnerability Assessment, Blackout Prevention, and Resilience Enhancement in Promoting Sustainable Energy Practices

Dan Codrut Petrilean , Nicolae Daniel Fita * , Gabriel Bujor Babut , Mila Ilieva Obretenova , Andreea Tataru , Sorina Daniela Stanila , Ioan Lucian Doidiu , Monica Crinela Burdea , Cruceru Emanuel Alin , Marius Manafu , Alexandru Radu

Posted Date: 14 October 2025

doi: 10.20944/preprints202510.1006.v1

Keywords: smart grid; vulnerabilities; blackout; resilience; sustainability

doi:10.20944/preprints202510.1006.v1

Article

Integrated Approaches for SG Management: Analysis, Vulnerability Assessment, Blackout Prevention, and Resilience Enhancement in Promoting Sustainable Energy Practices

Dan Codrut Petrilean [1], Nicolae Daniel Fita [1,*], Gabriel Bujor Babut [1], Mila Ilieva Obretenova [2], Andreea Tataru [1], Sorina Daniela Stanila [1], Ioan Lucian Doidiu [3], Monica Crinela Burdea [1], Cruceru Emanuel Alin [4], Marius Manafu [4] and Alexandru Radu [1]

[1] University of Petrosani, Romania
[2] University of Mining and Geology St. Ivan Rilski Sofia, Bulgaria
[3] Lucian Blaga University of Sibiu Sibiu, Romania
[4] University Politehnica of Bucharest, Romania
* Correspondence: daniel.fita@yahoo.com

Abstract

This study explores integrated methods for managing Smart Grid (SG) with a focus on complex vulnerability analysis, blackout prevention and increasing the resilience of energy infrastructure. In the context of the transition to renewable sources and increasingly stringent sustainability requirements, SG are becoming essential for optimizing consumption, reducing losses and ensuring the continuity of electricity supply. The paper highlights the importance of systematic risk assessment, including both physical threats and cyber-attacks, and proposes real-time monitoring methodologies for rapid detection and isolation of faults. By integrating IoT (Internet of Things), AI (Artificial Intelligence) and advanced predictive analytics technologies, it aims to prevent blackouts and reduce their impact on consumers. It also discusses strategies for increasing the resilience of SG, such as the implementation of autonomous micro-grids, energy storage and optimization of energy flows. The study highlights those integrated approaches that not only improve grid security and reliability, but also significantly contribute to promoting energy sustainability practices, through efficient use of resources and reducing the carbon footprint. The results highlight that proactive planning, combined with advanced monitoring and control technologies, allows SG to respond adaptively to disruptions, minimize risks and ensure a more sustainable and resilient energy system.

Keywords: smart grid; vulnerabilities; blackout; resilience; sustainability

---

1. Introduction

SG are modern electricity generation, transmission, and distribution systems that fuse digital technologies, communications, and automation with the legacy grid to optimize how power is produced, routed, and used—delivering efficiency, flexibility, and resilience at scale [1–4].

In practice, they rely on pervasive sensing with SCADA (Supervisory Control and Data Acquisition) and related telemetry for real-time monitoring and control, enabling operators to spot anomalies and manage flows as they happen, while newer intrusion-detection methods are being designed specifically for SCADA traffic in substations [5]. Automation then adjusts operating parameters (e.g., voltage/frequency) and supports predictive maintenance and self-healing behaviors, increasingly powered by AI for fast decision-making [6]. A core role of SG is to integrate variable renewables (solar, wind) and distributed resources alongside storage, coordinating them to maintain stability and reliability [1,7]. On the demand side, advanced metering and dynamic tariffs enable demand response and efficiency programs that modulate consumption in near real time [8]. These capabilities ride on two-way communications—between utilities, prosumers, and devices—most notably through advanced metering infrastructure that supports real-time exchange and control [3]. Finally, because the grid is now a cyber-physical system, resilience and security are first-order goals: recent work emphasizes cyber-resilient architectures and defenses for industrial control communications to detect, withstand, and recover from failures or cyberattacks [7–10].

The main components of SG encompass critical energy infrastructure—power plants, substations, and overhead, underground, or submarine power lines—forming the physical backbone that digital layers build upon to enhance reliability and sustainability [11]. Sensors and measurement devices include smart meters that record consumption in real time and transmit data to operators, alongside network sensors that track voltage, current, and frequency to prevent faults and optimize distribution [4]. Communication systems enable secure data exchange among plants, substations, consumers, and operators via wired and fiber networks, Power Line Communications (PLC), and wireless links such as LTE/5G and ZigBee [12,13]. SCADA control and automation systems monitor and operate equipment remotely, detecting and isolating faults to reduce outages and support self-healing behaviors in distribution networks [14]. Energy sources and storage integrate renewable generation (solar, wind, thermal, etc.) with grid-scale and distributed batteries to balance supply and demand while maintaining system stability [15]. Smart consumers and devices—across homes, buildings, and factories—can automatically adjust usage and participate in demand response, reducing consumption during peak periods (including EV/V2G - Electric Vehicle / Vehicle to Grids programs) through dynamic pricing and automation [15,18]. Finally, analytics platforms and software process grid data for optimization, forecasting, and preventive maintenance, increasingly using AI and machine learning to improve efficiency, resilience, and cyber-situational awareness [19].

The energy transition is the shift from fossil-fuel-dominated systems to renewable, efficient, low-carbon energy, driven by rapid CO_2 reduction in line with Paris Agreement goals, a rising share of renewables in the mix, stronger end-use and system-level efficiency, and diversification that boosts energy security and resilience [20]. Reducing CO_2 emissions remains urgent for climate mitigation, and recent studies show policy frameworks inspired by the Paris Agreement catalyze decarbonization pathways across sectors and regions [21,22]. Increasing the share of wind, solar, hydro and other green sources is central to national strategies, with recent analyses indicating that treaty-driven commitments and corporate instruments (e.g., PPAs/RECs - PPA — Power Purchase Agreement/ Renewable Energy Certificate) accelerate deployment [23].

Energy efficiency extents both consumption and grids: beyond end-use optimization, cutting technical and non-technical losses in transmission and distribution is essential, with new reviews and AI-based methods improving detection, forecasting and management of network losses.

Diversification and energy security (especially in Europe) reduce dependence on major fossil suppliers and enhance systemic resilience, with recent assessments highlighting the role of renewables, infrastructure modernization and innovation [24].

Altogether, the transition aims to deliver reliable, affordable power while decarbonizing, and 2024–2025 scenario syntheses emphasize rapidly rising electricity demand and the need to redirect capital toward grids, storage and flexibility to keep goals on track [25].

The energy transition faces well-known challenges—chief among them the intermittency of wind and solar resources, the consequent need for energy storage and system flexibility, and the adaptation of legacy infrastructure to new requirements—while grid digitalization integrates IT and communications into electricity networks to transform traditional grids into SG that more efficiently manage production, transport, and consumption [26–31]. In practice, digitalization raises energy efficiency and lowers operating costs via data-driven operations and predictive maintenance, strengthens stability and resilience through enhanced situational awareness and automation, and accelerates the shift to green energy by enabling large-scale renewable integration and coordination across time and space [1,29,30]. It is therefore important to the transition: it supports massive integration of intermittent renewables through better coordination, interconnection and planning

 doi:10.20944/preprints202510.1006.v1

[31]; expands storage and flexibility options—from long-duration energy storage and hybrid storage systems to smart electric vehicles and V2G services—so supply and demand can be balanced across hours to seasons [25,26,32–34]; reduces technical and non-technical losses and optimizes consumption using advanced metering, analytics and AI [29]; and increases visibility and control of power flows via digital-twin/ADMS (Advanced Distribution Management System)-style platforms that fuse operational and IT data [35].

SG link sustainability and energy security by embedding pervasive sensing, bidirectional communication, and automation into electricity systems so they can integrate variable renewables at scale while maintaining reliability and efficiency. In practice, digital monitoring and control across generation, networks, and end-use enable efficient renewable integration and lower CO_2 intensity, while analytics on smart-meter data support loss reduction, asset health, and operational optimization [36]. Conservation-voltage/volt-VAR optimization and related voltage-control schemes reduce technical losses and energy use at the distribution level, complementing analytics-based detection of non-technical losses (e.g., theft) to curb waste [37]. Demand-side flexibility—via dynamic tariffs, demand-response programs, and price-based scheduling—shifts consumption away from peaks, improves system adequacy, and reduces balancing costs, strengthening both sustainability and security [38–40]. Electrified mobility contributes as well: smart charging and V2G services turn EVs into flexible storage that can stabilize local grids and absorb renewable surpluses with minimal emissions impact [26]. At system scale, long-duration energy storage increases flexibility and resilience under prolonged wind/solar lulls ("renewables droughts"), reducing curtailment and dependence on carbon-intensive backup or imports [41]. On the security side, automated FLISR (Fault Location, Isolation and Service Restoration) and advanced outage-location methods accelerate recovery; microgrids add islanding capability for continuity during disturbances; and modern cybersecurity and anomaly-detection approaches mitigate evolving threats in increasingly digital grids [42–44]. Together, these capabilities reduce losses, optimize consumption, accommodate intermittent renewables, and harden infrastructure—making SG a cornerstone of a sustainable, resilient, and secure energy transition [37].

Integrating SG into sustainability goals is essential to accelerate a clean, efficient, and resilient energy system: recent research shows that digitalized grids directly support Sustainable Development Goals as SDG 7 (Affordable and Clean Energy), SDG 9 (Industry, Innovation and Infrastructure), and SDG 13 (Climate Action) by enabling higher renewable penetration, data-driven operation, and system resilience [1,37].

In practice, advanced monitoring and analytics (AMI - Advanced Metering Infrastructure, smart-meter data science) together with voltage/VAR (Volt-Ampere Reactive) control and conservation-voltage-reduction schemes curb technical losses and shave peaks—actions that translate into measurable CO_2 reductions from avoided generation and deferred grid reinforcements [45]. On the demand side, smart meters coupled with dynamic tariffs and demand-response programs shift consumption to hours with renewable surpluses, improving energy efficiency and lowering system costs while easing pressure at peak times [36]. Grid digitalization also underpins predictive maintenance and new service platforms (e.g., SGAM- Smart Grid Architecture Model compliant community energy systems), cutting O&M - Operations & Maintenance costs, fostering innovation, and strengthening critical infrastructure—key elements of SDG 8/9 [46]. Finally, SG make cities more sustainable and secure (SDG 11) by empowering prosumers and energy communities—through two-way communication, local storage, and peer-to-peer trading—to participate in balancing, flexibility, and local decarbonization while enhancing reliability at the edge of the network [47].

The main objectives of this work are:

- Smart-grid analysis in order to map and compare architectures, control layers, data flows, and interfaces between legacy assets and DERs (Distributed Energy Resources) to explain operating mechanisms and classical–renewable interactions.

 doi:10.20944/preprints202510.1006.v1

- Vulnerability identification and assessment with the aim to build a risk taxonomy (technical, cyber, operational) and a quantitative scoring model to prioritize threats to safety and stability.
- Blackout-prevention methods to design proactive tools (forecasting, protection coordination, DER/DR Distributed Energy Resources/ Demand Response pre-positioning) and reactive schemes (FLISR, UFLS/UVLS - Underfrequency Load Shedding/ Undervoltage Load Shedding, microgrid islanding) to reduce major-outage risk.
- Resilience enhancement in order to develop models and strategies that increase absorptive, adaptive, and restorative capacity to ensure service continuity under extreme or unforeseen events.
- Energy sustainability promotion with the aim to embed low-carbon best practices (CVR/VVO - Conservation Voltage Reduction/ Volt/VAR Optimization, DR, storage orchestration) to cut losses and carbon intensity while optimizing consumption.

Authors' contributions in this work consists of:

- Integrated conceptual framework for a multidisciplinary, SGAM-aligned framework uniting power-systems engineering, cybersecurity, and sustainability for end-to-end analysis.
- Vulnerability assessment methodology with measurable criteria and indicators, plus a reproducible scoring toolkit, for risk analysis specific to SG.
- Innovative blackout-prevention solutions using AI-driven forecasting and anomaly detection with automation (ADMS/DERMS - Distributed Energy Resources Management System) to prevent cascading failures and speed restoration.
- Resilience strategies are models for co-optimizing generation–storage–demand, orchestrating microgrids, and sequencing restoration to minimize EENS (Expected Energy Not Served) and recovery time.
- Energy-sustainability advances in order to emphasize actionable recommendations and policy–technology playbooks for integrating renewables and efficiency measures into routine grid operations.

2. State of the Art and Sector Landscape

2.1. International Landscape

Internationally, regulation and assessment of cyber-risk in the energy sector are accelerating. In the EU, the new Network Code on Cybersecurity (Delegated Reg. (EU) 2024/1366) sets sector-specific rules for cross-border electricity flows—covering common minimum requirements, planning, monitoring, reporting, and crisis management—while NIS2 is being implemented with technical guidance and sector maturity baselining from ENISA (NIS360). In parallel, operators are deploying real-time monitoring and rapid detection/mitigation (e.g., PMUs per IEEE C37.118, Wide-Area Monitoring System WAMS/EMS/DMS, dynamic state estimation, automated reconfiguration) to reduce instability and prevent wide-area collapses. Recent events on 28 April 2025 in the Iberian Peninsula (currently under ENTSO-E expert investigation) underscore that cascading outages remain a live risk. Early official statements point to voltage oscillations rather than a cyberattack, and remedial lessons are being folded into EU and TSO plans [48].

The global picture today:

1. Regulation and security frameworks

 doi:10.20944/preprints202510.1006.v1

- EU publishes specific codes for cybersecurity in the electricity sector (Network Code on Cybersecurity) adopted in March 2024 and steps up enforcement of NIS2. ENISA provides maturity analyses (NIS360) for critical sectors. These impose requirements for risk assessment, vulnerability reporting and supply chain management [49];
- In North America NERC CIP standards (FERC-approved and evolving) remain the mandatory baseline for the Bulk Electric System. FERC continues to update/strengthen CIP (e.g., CIP-003-11 proposals in 2025) [50];
- UK applies NIS Regulations for downstream gas/electricity with Ofgem as co-competent authority and statutory guidance for Operators of Essential Services [51];
- Australia with SOCI/SLACIP regime expands mandatory risk-management and reporting obligations across critical infrastructure (incl. electricity) [52];
- Singapore implements Cybersecurity Act (amended 2024/2025) that sets obligations for Critical Information Infrastructure, including the energy sector [53];
- Global standards ecosystem relies on IEC 62351 series for power-system communications security and ISO/IEC 27019:2024 for energy-utility controls complement regulatory frameworks. IEC 62351-3:2023 stipulates how to provide CIA confidentiality, integrity availability, and message level authentication for protocols that make use of the TCP/IP protocol (OSI Transport Layer) where cyber-security is compulsory [54]. ISO/IEC 27019:2024 standard rules about information security controls for the energy utility industry [55].

2. Emerging technologies

Utilities/TSOs are expanding wide-area, real-time monitoring and control: PMUs (per IEEE C37.118) feed WAMS and advanced EMS/DMS. Dynamic state estimation (DSE) improves observability and early instability detection. Orchestration of DERs/ESS via DERMS/ADMS supports fast reconfiguration and frequency/voltage support. Evidence from standards bodies, laboratories, and reviews shows significant gains in situational awareness, oscillation detection, and stability margins with PMU-enabled analytics and DSE, and reliability benefits from DER orchestration [56].

3. Lessons from recent incidents

The event produced a large-scale loss of supply across Spain and Portugal with knock-on effects; early communications from grid operators and ministries ruled out a cyberattack and pointed to voltage/frequency oscillations and protection interactions, while ENTSO-E's expert panel continues publishing findings and convening stakeholders. EU and national authorities are already acting on interconnection and resilience gaps highlighted by the blackout [57–73].

2.2. Romanian National Landscape

Romania applies policies and plans (Transelectrica, distributors' investments) for the introduction of SG elements, but efforts on vulnerability assessments, standardization and full-scale testing need to be intensified.

4. Policies and plans - Transelectrica company has included the development of SG elements in the RET Development Plan 2024–2033; large companies (such as Electrica etc.) are investing in monitoring and digitalization of networks. However, large-scale implementation of advanced functions (PMU, extended DMS automation, DER integration) by DSO/TSO is ongoing;
5. Vulnerability assessment capacity - existence of studies and activity reports by private/sectoral actors, but lack of frequent publications of independent audits and national resilience testing programs to cyber-attacks and extreme scenarios;
6. EU funding & programs - Romania can access EU funds for smart-grid modernization (included in operational programs) — opportunity to increase DSO/TSO capabilities;

 doi:10.20944/preprints202510.1006.v1

7. Vulnerability assessment:

- Cyber vulnerabilities - compromised inputs (SCADA/RTU/IED), vulnerable firmware, supply chains, unencrypted telemetry, lack of segmentation of operational networks. ENISA and industry events recommend periodic assessments, OT-specific pen-testing and vulnerability management;
- Physical/operational vulnerabilities - loss of regulation capacity (inertia reduction due to high penetration of renewables), protection failures, lack of back-ups for critical communications. Recent studies show that climate change increases the risk of outages.

8. Blackout prevention techniques and practices:

- Advanced monitoring: PMU, dynamic state estimation, real-time anomaly detection and RT-NMS for automated actions;
- Systemic services and market design: preserving control capabilities (synchronous resources, fast reserve, balancing contracts), progressive disconnection rules;
- Distributed operation and microgrids: islanding/local control capability of DER + storage reduces the risk of extended power outage;
- Restoration plans and exercises: scale simulations, coordinated exercises TSO-DSO-Suppliers-Authorities. ENTSO-E and regional bodies promote post-incident investigations and peer learning.

9. Resilience measures (medium-long term):

- Segmentation and redundancy of communications (separate fiber + LTE/5G channels); encryption & strong authentication for IED/SCADA;
- Operational flexibility: integration of batteries and DER with VPP controllers/aggregators for rapid response;
- Proactive vulnerability management: software/hardware inventory, patch management and transparent reporting (according to NIS2 / network code);
- Climate capabilities: design with extreme event scenarios (maximum loads, temperatures) and infrastructure modernization for overloads.

10. Recent lessons and trends:

• Major blackouts can start from multi-factor technical combinations (voltage, protections, generation loss). There are not always cyber-attacks. The response is strengthening physical monitoring and cybersecurity;

• European regulations are evolving rapidly, and energy entities must integrate NIS2 requirements and sector codes into procedures and contracts.

11. Practical recommendations for Romania (priority):

• National vulnerability assessment program (OT/IT audit, pen-testing, soft/hardware inventory) — coordinated by TSO + DSO + Authority (ANRE/Transelectrica);

• Rapid implementation of PMU/State Estimation at critical nodes and data integration at TSO-DSO level for early detection;

• National blackout exercises (tabletop combined with practical exercises) with scenarios inspired by the Iberian case and other recent events. These include telecommunications and critical services;

• EU program funding plan for DMS, SCADA and resilient communications modernization (to be used lines from PNRR/POIM/other);

 doi:10.20944/preprints202510.1006.v1

• Creation as well as participation in regional vulnerability information exchange mechanisms in order to keep sharing threat intelligence updated according to ENISA.

2.3. Academic Scientists

International specialists:

• Prof. Massoud Amin – University of Minnesota. Recognized expert in security, resilience and self-healing for SG;

• Prof. Enrico Zio – Politecnico di Milano / ETH / research in reliability, vulnerability and uncertainties for energy systems (smart grid vulnerability studies);

• Dr. Daogui Tang – research on "false pricing" / social-network-based attacks on smart grid demand-response programs;

• Prof. Yi-Ping (Yiping) Fang – CentraleSupélec / Université Paris-Saclay; work on computational models for risk, vulnerability and resilience analysis of critical infrastructures (including SG);

• Prof. José E. Ramírez-Márquez – Stevens Institute of Technology; specialist in systems resilience and quantitative assessments of infrastructure vulnerability/resilience;

National specialists:

• Prof. Dan Popescu – Politehnica University of Bucharest (Automatics / Systems) — involved in relevant fields for measurement, control and smart-grid applications;

• Prof. Sorin-D. Grigorescu – research in electrical engineering, power quality monitoring and applications for SG;

• Prof. Ciprian Dobre – Politehnica University of Bucharest (academic profile/activity; IT and systems fields) — relevant contributions to IT/telecom components of smart-grid;

• Dr. Radu Plămănescu – Politehnica University of Bucharest (measurements and data platforms for SG) — works and projects related to practical applications in grids.

3. Vulnerability Assessment

Vulnerability assessment of SG is essential to ensure their security, reliability and efficiency. SG integrate information and communication technology with energy infrastructure, which makes them more efficient, but also more vulnerable to cyber-attacks, technical errors or natural disasters. [74,75].

Here are the main aspects that emphasize the importance of vulnerability assessment: protection against cyber-attacks, increasing system reliability, optimizing risk management, compliance with regulations and standards, improving operational efficiency and preparedness for incidents and rapid recovery.

Vulnerability assessment of SG is not only a security measure, but an essential practice for protecting critical infrastructure, ensuring service continuity and optimizing performance. The lack of this assessment can lead to significant economic losses, social problems and compromises in national security.

Vulnerability Assessment: Poor management of the transmission operator activity (operation, maintenance and development) on the energy installations related to the Electricity Transmission Network: 110 kV – 400 kV power station → Technical failure / Associated technical incident → Blackout.

A. Root-Cause and Effect Analysis

Table 1. Analyzes the causes of the identified vulnerabilities.

Vulnerability identified	Identification of the generated source (Dysfunction, deficiency, non-conformity)	Causal analysis

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 October 2025 doi:10.20944/preprints202510.1006.v1

Poor management of the transmission operator activity (operation, maintenance and development) of energy installations related to the Electricity Transmission Network	Dysfunction	• lack, precariousness or non-compliance with operating procedures; • lack, precariousness or non-compliance with maintenance procedures; • lack, precariousness or non-compliance with development procedures.

Table 2. Analyzes the effects of the identified vulnerabilities.

Causes	Effects
• short circuits of power equipment; • loads of some overhead power lines; • loads of some power equipment; • poor condition of power equipment; • lack of investment in power stations; • non-functioning of system automation within power groups; • lack of overhauls of power equipment; • lack of upgrading of power stations; • incorrect configuration of power stations; • lack of specialized and/or trained operational personnel; • lack of communication or poor communication with DET – Territorial Power Dispatcher or DEN – National Power Dispatcher; • unspecialized DET or DEN personnel during a crisis; • lack of work procedures in power stations during a crisis; • lack / non-compliance / ignorance of national / European procedures in case of serious damage (black out); • lack of training in the field of Risk Management; • failure to close the 400 kV ring of Romania – becomes a vulnerability of the SEN – National Energy System; • occurrence of electrical discharges; • lack or incorrect functioning of lightning rod installations; • incorrect functioning of arresters; • failure to comply with fire safety regulations; • failure to comply with occupational health and safety regulations; • failure to use PPE – Personal Protective Equipment; • poor condition of energy equipment; • lack of overhauls of energy equipment; • use of non-compliant energy subassemblies; • lack of investments; • failure to modernize electrical substations; • lack of specialized and/or trained maintenance personnel; • wrong maneuvers performed by operational personnel in substations.	• stopping the energy market between Romania and the EU (ENTSO-E); • stopping the energy market between Romania and Serbia, Ukraine, the Republic of Moldova; • failure to supply electricity to neighboring energy systems and the EU; • failure to supply electricity to important consumers and to the main power lines within the SEN; • possibility of a local, regional or national blackout. • work accidents caused by an explosion that may generate fire (individual or collective) fatal or with incapacity for work; • work accidents caused by a fire (unitary or collective) fatal or with incapacity for work; • propagation of the explosion (fire) to other energy equipment in the area; • propagation of the explosion (fire) to other external objectives (forests, houses, blocks of flats, factories, etc.); • propagation of the fire to other energy equipment in the area; • spread of the fire to other external objects (forests, houses, blocks of flats, factories, etc.); • untimely disconnection of the respective equipment; • material damage resulting from the lack of electricity; • major material damage resulting from the interdependence of other consumers

B. Situational Severity Analysis

Table 3. Analyzes the situational severity.

doi:10.20944/preprints202510.1006.v1

<table>
<tr><th>Situational Severity Analysis</th><th>Level</th></tr>
<tr><td rowspan="5">a) Failure to close Romania's 400 kV ring:
• lack of investment (failure to upgrade power stations, overhead power lines and new energy objectives);
• impregnability of the political system;
• possibility of a zonal, regional or national blackout, generating the shutdown of the electricity market between Romania and the EU;
• economic insecurity generating national insecurity;
b) Specialization degree and periodic training of personnel responsible for restoring the electricity supply process:
• operational personnel;
• maintenance personnel;
• security personnel.
c) Location of the power station (European critical infrastructure) from the point of view of safety in supplying electricity to consumers:
• zonal, regional and national consumers;
• national interconnection;
• interconnection with neighboring energy systems.
d) Degree of specialization and training of fire response personnel;
e) Degree of specialization and periodic training of operational personnel responsible for restoring the electricity supply process;
f) Equipping the power station with fire extinguishing means and equipment;
g) Equipping the operational personnel with individual means and protective equipment;
h) Existence of work procedures in the field of security for the power station:
• risk management;
• crisis management;
• emergency management;
• occupational health and safety management.
i) State of equipment and technological installations related to the electricity transmission process (lack of investment):
• protection equipment against atmospheric overvoltages (lightning rods, arresters);
• transformation equipment (transformers, autotransformers);
• switching and protection equipment (circuit breakers, disconnectors);
• insulators, measuring transformers (voltage and current), etc.;
• technical and human resilience:
partial or total technical possibility of returning to the initial state;
partial or total human possibility of returning to the initial state.</td><td>1. Very low</td></tr>
<tr><td>2. Low</td></tr>
<tr><td>3. Medium</td></tr>
<tr><td>4. High</td></tr>
<tr><td>5. Very high</td></tr>
</table>

C. Severity Level

Table 4. Analyzes the severity level.

Level	Severity
1. Very low	The event causes minor disruption to business operations, with no material damage
2. Low	The event causes minor material damage and limited disruption to business operations

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 October 2025 doi:10.20944/preprints202510.1006.v1

	3. Medium	Injuries to personnel, and/or some loss of equipment, utilities, and delays in service provision.
	4. High	Serious injuries to personnel, significant loss of equipment, facilities, and delays and/or interruption of service provision.
X	5. Very high	The consequences are catastrophic resulting in fatalities and serious injuries to personnel, major loss of equipment, facilities, and services, and interruption of service provision.

D. Impact Analysis

Table 5. Analyzes the impact.

Impact Analysis	Level		
Potential deaths (persons)	X	1. Very low	0 – 5 persons
		2. Low	6 – 10 pers.
		3. Medium	11 – 15 pers.
		4. High	16 – 20 pers.
		5. Very high	> 21 pers.
Potential injured persons (persons)	X	1. Very low	0 – 20 pers.
		2. Low	21 – 40 pers.
		3. Medium	41 – 60 pers.
		4. High	61 – 80 pers.
		5. Very high	> 81 pers.
Potential damage or deterioration of on-site infrastructures providing the main utilities: electricity, communications, drinking water, natural gas (damages)		1. Very low	Temporary damage
		2. Low	Temporary damage
		3. Medium	Average damage
		4. High	High damage
	X	5. Very high	Very high damage
Potential damage or deterioration of the material assets of those served by the national critical infrastructure in question: public, commercial, private (return on invested capital)		1. Very low	0 – 10% of VCI
		2. Low	11 – 20% of VCI
		3. Medium	21 – 30% of VCI
		4. High	31 – 40% of VCI
	X	5. Very high	over 41% of VCI
Potential damage or deterioration of the environment (%)		1. Very low	0 – 20%
		2. Low	21 – 40%
	X	3. Medium	41 – 60%
		4. High	61 – 80%
		5. Very high	over 81%
Potential social impacts (population confidence)		1. Very low	0 – 10% din ÎP
		2. Low	11 – 20% of ÎP
	X	3. Medium	21 – 30% of ÎP
		4. High	31 – 40% of ÎP
		5. Very high	peste 41% of ÎP

E. Impact Level

Table 6. Analyzes the impact level.

Nivel	Impact
1. Very low	The event causes minor disruption to business operations, with no material damage

	2. Low	The event causes minor material damage and limited disruption to business operations
	3. Medium	Injuries to personnel, and/or some loss of equipment, utilities, and delays in service provision.
	4. High	Serious injuries to personnel, significant loss of equipment, facilities, and delays and/or interruption of service provision.
X	5. Very high	The consequences are catastrophic resulting in fatalities and serious injuries to personnel, major loss of equipment, facilities, and services, and interruption of service provision.

F. Identification of critical equipment involved

The critical equipment involved consists of:

- Overhead power lines;
- High power (auto) transformers;
- Circuit breakers, isolators;
- Compensation coils, reactors, quenching coils;
- Current and voltage transformers (measuring devices);
- Arrester, fuses (protective devices);
- Conductors, insulators.

G. Interdependencies Analysis

Table 7. Analyzes the interdependencies created.

Interdependencies Analysis	Infrastructure or critical systems
• drinking water supply system; • natural gas system; • oil system; • mining system; • nuclear system; • economic system; • transportation system; • information system; • financial-banking system; • industrial system, etc	• aqueducts, pumping stations, etc.; • gas pipelines, pumping stations, etc.; • oil pipelines, pumping stations, etc.; • coal mines; • nuclear, hydroelectric, thermoelectric power plants, etc.; • airports, airplanes, stations, trains, highways, ports, ships, etc.; • banks; • industrial systems, etc.

H. Calculation of the Vulnerability Level (vulnerability matrix)

GRAVITY						
	Very high 5					Scenario 1
	High 4					
	Medium 3					
	Low 2					
	Very low 1					
	0	Very low	Low	Medium	High	Very high

		1	2	3	4	5
IMPACT						
Note: The vulnerability level is given by the product of the severity level x the impact level						

The calculated vulnerability has the value
25
(Severity 5 x impact 5)
therefore, there is a
VERY HIGH
vulnerability level of the chosen scenario

VULNERABILITY LEVEL CALCULATED		
	Level	SCORE
	Very low	1 – 3
	Low	4 – 6
	Medium	7 – 12
	High	13 – 16
X	Very high	17 – 25

I. Proposed Recommendations

Table 8. Exemplifies the proposed recommendations.

Vulnerability	Recomandations proposed
Failure to close Romania's 400 kV ring	• major investments in national and European critical infrastructure; • predictability (security) of the political system; • accessing European funds regarding the security of European critical infrastructures.
The degree of specialization and periodic training of operational personnel responsible for restoring the electricity supply process	• training and advanced training courses for operational, maintenance and security personnel; • analysis of events, incidents, etc.; • control of installations on the operating line and carrying out preventive maintenance.
The degree of specialization and training of fire response personnel	• training and advanced training courses in the field of emergency situations - PSI; • simulations of interventions (very short time) in case of fires.
Equipping the power station with fire-fighting means and equipment	• provision of individual fire-fighting means and equipment.
The state of technological equipment and installations related to the electricity transmission process (lack of investment)	• major investments in high-performance equipment.

Table 9. Analyzes the level of vulnerability according to the proposed recommendations.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 October 2025 doi:10.20944/preprints202510.1006.v1

Vulnerability	Identified	After the proposed recommendations
a) Failure to close the 400 kV ring of Romania;	1. Very low	1. Very low
b) Degree of specialization and periodic training of operational personnel responsible for restoring the electricity supply process;	2. Low	2. Low
	3. Medium	X 3. Medium
	4. High	4. High
c) Degree of specialization and training of fire response personnel; d) Degree of specialization and periodic training of operational personnel responsible for restoring the electricity supply process; e) Equipping the power station with fire-fighting means and equipment; f) Location of the power station (European critical infrastructure) in terms of safety in supplying consumers with electricity; g) Equipping the operational personnel with individual means and protective equipment; h) Existence of work procedures in the field of security for the power station: i) State of equipment and technological installations related to the electricity transport process (lack of investment); j) Technical and human resilience.	X 5. Very high	1. Very high

J. Recalculation of the Vulnerability Level (vulnerability matrix)

GRAVITY					
Very high 5			Scenario 1		
High 4					
Medium 3					
Low 2					
Very low 1					
0	Very low 1	Low 2	Medium 3	High 4	Very high 5
			IMPACT		

Note: The vulnerability level is given by the product of the severity level x the impact level

The calculated vulnerability has the value 15 (Severity 5 x impact 3) therefore, there is a MEDIUM vulnerability level of the chosen scenario

VULNERABILITY LEVEL CALCULATED	
Level	SCORE
Very low	1 – 3
Low	4 – 6

X	Medium	7 – 12
	High	13 – 16
	Very high	17 – 25

4. Blackout Prevention, Resilience Assessment and Quantification

4.1. Blackout Prevention

A blackout (total power failure over large areas) can be prevented through a set of technical, organizational and behavioral measures, both at the level of system operators and consumers. Here are some main directions:

c) At the energy system level:

- Infrastructure modernization by replace the power lines (overhead, underground or submarine) of old and obsolete (auto)transformers and distribution equipment (poor and/or non-compliant condition) to reduce the risk of failure;
- Automation and protections by implement novel SCADA systems and automatic protections that can quickly isolate the affected areas, without interrupting the entire network;
- Reserve capacities by maintain plants on standby (hydro, gas, large batteries) that can be started quickly when needed;
- Diversification of energy sources using a smart and reliable balanced integration of renewable sources with storage (batteries, hydro-pumping) and maintaining stable capacities (nuclear, hydro, gas);
- International interconnections allowing connecting to the electricity networks of other countries for mutual support in case of imbalance;
- Testing and exercises including regular simulations for major breakdown scenarios and clear restart procedures ("black start").

d) At the level of industrial consumers:

- Backup generators to maintain critical activity;
- Consumption management (demand response) to reduce or shift consumption during peak hours;
- Protection equipment (UPS, stabilizers) to avoid failure of equipment sensitive to fluctuations.

e) At the level of household consumers:

- Reducing consumption during peak hours (morning/evening, summer/winter);
- Energy-efficient equipment and rational use of large household appliances;
- Alternative sources as portable batteries, solar panels with storage, small generators for emergency situations;
- Awareness as a main tool for an educated population about how to react and how to temporarily reduce consumption in critical situations.

Preventing a blackout means balance between production and consumption, a modern and flexible network, plus cooperation between operators and users.

Table 10. Exemplifies the cause of the occurrence and propagation of a blackout.

Scenario	Cause of production and propagation

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 October 2025 doi:10.20944/preprints202510.1006.v1

Black-out	1. Faults in the Electric Transmission Network: • Interrupted overhead power lines: storm, ice, lightning, insulation defects, etc.; • Major short circuits; • Falling of some power stations: affects the balance between areas. 2. Imbalance between production and consumption: • If the production of electricity suddenly drops (e.g. shutdown of a high-power power plant), and consumption remains high, the frequency drops below 50 Hz → automatic trips → chain effect; • Unexpectedly high electricity consumption, or sudden variations without the possibility of rapid adjustment of production. 3. Power plant faults: • Sudden shutdown of a large power plant (hydroelectric, nuclear, thermal, etc.) → large loss of power; • Faults in the protection or automation systems of power plants. 4. Poor coordination in the National Energy Dispatching Office or territorial dispatching offices: • Wrong dispatching decisions (switching of important loads in an unsynchronized manner); • Lack of communication between regional operators of the NES or with neighboring states in case of interconnection. 5. Problems in protection and automation systems: • Protections that act incorrectly or with delay, which can propagate a fault; • Failure to perform the islanding or self-restoration function. 6. Cyber-attacks or computer errors • Attacks on SCADA or other IT systems that control the NES; • Software errors or hardware defects in control equipment. 7. Natural disasters or catastrophes: • Earthquakes, floods, fires affecting key equipment; • Extreme frosts causing lines to break or turbines to block.

4.2. Assessing and Quantifying the Resilience of SG

Table 11. Estimates resilience according to the blackout generating factor.

Factor generator – black-out	Resilience
1. Faults in the Electric Transmission Network: • Interrupted overhead power lines; • Insulation faults, etc.; • Major short circuits; • Fall of some electrical stations → affects the balance between areas; • Auto/transformer fault, reactor coil, extinguishing coil, circuit breaker, isolator, busbar, voltage/current transformer, insulator, etc.	• 5 – 25 hours*
2. Imbalance between production and consumption:	

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 October 2025 doi:10.20944/preprints202510.1006.v1

- If electricity production suddenly drops (e.g. shutdown of a high-power power plant), and consumption remains high, the frequency drops below 50 Hz → automatic trips → chain effect;
- Unexpectedly high electricity consumption, or sudden variations without the possibility of rapid production adjustment.

3. Power plant failures:

- Sudden shutdown of a large power plant (hydroelectric, nuclear, thermoelectric, etc.) → large power loss;
- Defects in the protection or automation systems of power plants.

4. Poor coordination in the National Energy Dispatching Office or territorial dispatching offices:

- Wrong dispatching decisions (switching of important loads in an unsynchronized manner);
- Lack of communication between regional operators of the SEN or with neighboring states in case of interconnection.

5. Problems in protection and automation systems:

• Protections that act incorrectly or with a delay, which can propagate a failure;

** depending on the blackout generator factor (type of fault), resilience can last less than 5 hours or more than 25 hours.*

Table 12. Approximates resilience according to the type of blackout.

Black-out type	Propagation area	Risk level*	Resilience
1. Local blackout	Apartment/home	1	5 – 20 minutes
2. Zonal blackout	Neighborhood	4	20 – 40 minutes
3. Rural/communal black-out	Village/commune	6	40 – 60 minutes
4. Urban blackout	City/district	12	1 – 2 hours
5. Regional blackout	Region	16	2 – 5 hours
6. National blackout	Whole country	5	5 – 25 hours
7. Continental blackout	Continent	5	10 – 50 hours
8. Intercontinental blackout	Continents	5	20 – 100 hours

* RISK LEVEL	
Level	Score
Very Low	1 – 3
Low	4 – 6
Medium	7 – 12
High	13 – 16
Very high	17 – 25

The resilience (exposure time) was approximated by the authors following statistics of fault times (technical incidents) within the SEN Electricity Transmission Network.

Table 13. Exemplifies the key elements that make up national resilience and their impact on national security.

Key elements of national resilience	Impact on national security	Importance on national security
1. Institutional capacity: Functionality and robustness of government, public administration, army, police, etc.;	1. Very low 2. Low 3. Medium 4. High	Maintains the functioning of state and societal mechanisms and institutions under stress

 doi:10.20944/preprints202510.1006.v1

Inter-institutional coordination in emergency situations.	5. Very High	
2. Critical infrastructure: Safety and functioning of transport, energy, water, telecommunications networks; Continuity plans in case of major breakdowns.	1. Very low 2. Low 3. Medium 4. High 5. Very High	Provides essential facilities for the population and reduces the negative impact of external or internal shocks
3. Crisis response: Early warning and rapid response systems; National disaster and pandemic response plans.	1. Very low 2. Low 3. Medium 4. High 5. Very High	Increases the capacity for rapid and effective recovery after a crisis
4. Economy and finance: Economic recovery capacity; Strategic reserves and fiscal stability.	1. Very low 2. Low 3. Medium 4. High 5. Very High	Increases the capacity for economic recovery after a crisis
5. Societal dimension: Social cohesion, trust in institutions, civic education; Resistance to disinformation and propaganda.	1. Very low 2. Low 3. Medium 4. High 5. Very High	Strengthens the security and societal stability of the population
6. Security and defence dimension: Military capacity, reservist mobilization, NATO/EU cooperation; Border protection and cybersecurity.	1. Very low 2. Low 3. Medium 4. High 5. Very High	Provides essential military facilities to the army and national safety and security structures
7. Sustainability and climate change: Adaptation to medium-risk, natural resource management; Green energy transition strategies.	1. Very low 2. Low 3. Medium 4. High 5. Very High	Provides essential resources for the population and reduces the negative impact of external or internal shocks
8. Energy, food and drinking water: Continuous access to energy: natural gas, oil, fuels (diesel, gasoline, kerosene, etc.), coal, uranium, etc.; Continuous access to food; Continuous access to drinking water.	1. Very low 2. Low 3. Medium 4. High 5. Very High	Provides essential resources for the population and reduces the negative impact of external or internal shocks

5. Strategies to Increase the Resilience ff SG and Promote Energy Sustainability Practices

5.1. Increasing the Resilience of SG

 doi:10.20944/preprints202510.1006.v1

SG are modern energy systems that integrate digital technology to optimize energy production, distribution and consumption. To be resilient, they must cope with shocks (natural disasters, cyberattacks, demand fluctuations).

a. Robust and flexible infrastructure:

- Modernization of transmission and distribution lines with weatherproof cables;
- Network redundancy (the possibility of rerouting energy in the event of failures);
- Distributed storage through batteries, hydrogen or other technologies.

b. Advanced digitalization and monitoring:

- Implementation of IoT sensors and smart meters for rapid anomaly detection;
- Use of artificial intelligence for consumption forecasts and failure prevention;
- Creation of control centers with self-healing algorithms (self-healing grids).

c. Cybersecurity and data protection:

- Implementation of cybersecurity standards to prevent attacks;
- Segmentation and encryption of network communications;
- Stress tests and periodic attack simulations.

d. Integration of distributed energy resources (DER):

- Decentralized production from renewable sources (solar panels, local wind);
- Independent microgrids that can operate in isolation in case of crisis;
- Prosumer models, where consumers are also energy producers.

5.2. Promoting Energy Sustainability

Following the identification of vulnerabilities within the Electric Transmission Network, the following recommendations with a stability, security and sustainability effect are recommended, according to table 14.

Table 14. Proposed recommendations with a stability, security and sustainability effect.

Vulnerabilities of the Electric Transmission Network	**Proposed recommendations with a stability, security and sustainability effect**
Non-closure of Romania's 400 kV ring	a) major investments in national and European critical infrastructure; b) predictability (security) of the political system; c) accessing European funds regarding the security of European critical infrastructures.
Degree of specialization and periodic training of operational personnel with duties of restoring the electricity supply process;	d) training and advanced training courses for operational, maintenance and security personnel e) analysis of events, incidents, etc.; f) control of installations on the operating line and carrying out preventive maintenance.
Degree of specialization and training of fire intervention personnel	g) training and improvement courses in the field of emergency situations - PSI; h) simulations of interventions (very short time) in case of fires
Equipping the power station with fire extinguishing means and equipment	i) equipping with individual fire extinguishing means and equipment
State of technological equipment and installations related to the electricity	j) major investments in high-performance equipment

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 14 October 2025 doi:10.20944/preprints202510.1006.v1

transmission process (lack of investments)	

The objective is to reduce the carbon footprint and use resources efficiently.

a. Transition to renewable sources:

- Increasing the share of solar, wind, geothermal and hydro energy;
- Fiscal incentives and support schemes for investments in renewables;
- Development of green energy storage capacities.

b. Energy efficiency:

- Implementation of smart buildings with efficient lighting and air conditioning systems;
- Modernization of industrial equipment and reduction of losses in the distribution chain;
- Education and awareness programs for consumers.

c. Green policies and regulations:

- Introduction of dynamic tariffs to encourage responsible consumption;
- Efficiency standards for electrical appliances and vehicles;
- Integration of climate neutrality objectives into national strategies.

d. Innovation and community participation:

- Peer-to-peer trading platforms for locally produced energy;
- Community renewable energy projects;
- Supporting research in emerging technologies (SMR, long-term storage, hybrid SG).

The resilience of SG is based on technology, security and flexibility, and energy sustainability on the green transition, efficiency and active participation of communities. Together, they ensure a secure, environmentally friendly and adaptable energy system.

6. Results

The paper highlighted the fact that SG are the foundation of the transition to a sustainable, secure and flexible energy system. By integrating digital technologies, renewable sources and advanced monitoring and control mechanisms, they become capable of responding to current challenges related to energy security and climate change.

The analysis carried out showed that identifying and assessing vulnerabilities is a critical step in reducing the risks of blackouts and ensuring the continuity of essential services. Preventive approaches, based on simulations, prediction algorithms and data management tools, contribute decisively to anticipating incidents and optimizing the response of networks in crisis situations.

At the same time, the importance of operational resilience was highlighted: not only the ability to withstand major disruptions, but also the ability to quickly return to normal operating parameters. The implementation of integrated governance frameworks, standardization and collaboration between actors – network operators, authorities, producers and consumers – is the key to increasing the robustness and adaptability of the system.

Promoting energy sustainability cannot be separated from these technical aspects. SG facilitate the integration of renewable sources, encourage energy efficiency and give consumers an active role in balancing supply and demand. Thus, the approaches presented demonstrate that an integrated strategy, based on technology, security and sustainability, is essential for strengthening the future of the energy sector.

Directions for future research:

a) Integrated analysis of SG:

 doi:10.20944/preprints202510.1006.v1

• Development of hybrid models (based on AI, ML and physical-mathematical simulations) for the forecast of energy consumption and production;

• Creation of digital twin platforms for simulating the behavior of the grid under normal and stress conditions;

• Integration of data from distributed sources (prosumers, storage, electric vehicles) for the optimization of energy flows.

b) Vulnerability and risk assessment:

• Development of standardized methodologies for assessing cyber and physical risks to SG;

• Analysis of interdependencies between electrical, communications and transport networks to identify critical points of vulnerability;

• Investigation of coordinated attack scenarios (cyber-physical) and development of rapid response protocols.

c) Blackout prevention and resilience enhancement:

• Implementation of algorithms for early detection of anomalies and instabilities in real time;

• Development of controlled islanding and self-configuration strategies for networks to limit the propagation of failures;

• Optimization of storage and load balancing mechanisms by integrating high-capacity batteries and autonomous microgrids.

d) Promotion of energy sustainability:

• Research on models for integrating distributed renewable sources into SG, with a focus on reducing losses and maximizing efficiency;

• Investigate the impact of flexible consumption and demand response practices on emission reduction and energy efficiency;

• Develop incentive-based policies and economic instruments for the large-scale adoption of sustainable technologies.

e) Interdisciplinary and collaborative approaches:

• Integrate knowledge from fields such as electrical engineering, data science, cybersecurity and energy economics;

• Create partnerships between academia, industry and policymakers to validate and implement proposed solutions;

• Promote pilot projects and testbeds to accelerate the transition to safer and more sustainable energy networks.

This work contributes to strengthening energy security, resilience and sustainability through a holistic approach that combines prevention, adaptability and sustainability, providing an applicable framework for the development and operation of modern SG.

References

1. Campana, P.; Censi, R.; Ruggieri, R.; Amendola, C. SG and Sustainability: The Impact of Digital Technologies on the Energy Transition. *Energies* 2025, 18, 2149. https://doi.org/10.3390/en18092149
2. Kiasari, M.; Ghaffari, M.; Aly, H.H. A Comprehensive Review of the Current Status of Smart Grid Technologies for Renewable Energies Integration and Future Trends: The Role of Machine Learning and Energy Storage Systems. *Energies* 2024, 17, 4128. https://doi.org/10.3390/en17164128
3. Faria, P.; Vale, Z. Demand Response in SG. *Energies* 2023, 16, 863. https://doi.org/10.3390/en16020863
4. Koukouvinos, K.G.; Koukouvinos, G.K.; Chalkiadakis, P.; Kaminaris, S.D.; Orfanos, V.A.; Rimpas, D. Evaluating the Performance of Smart Meters: Insights into Energy Management, Dynamic Pricing and Consumer Behavior. *Applied Sciences* 2025, 15, 960. https://doi.org/10.3390/app15020960
5. Yilmaz, S.; Dener, M. Security with Wireless Sensor Networks in SG: A Review. *Symmetry* 2024, 16, 1295. https://doi.org/10.3390/sym16101295
6. Dokku, N.S.; Raj, R.D.A.; Bodapati, S.K.; Pallakonda, A.; Reddy, Y.R.M.; Prakasha, K.K. Resilient Cybersecurity in Smart Grid ICS Communication Using BLAKE3-Driven Dynamic Key Rotation and Intrusion Detection. Scientific Reports 2025, 15, 32754. https://doi.org/10.1038/s41598-025-17530-z

7. Ejuh Che, E.; Roland Abeng, K.; Iweh, C.D.; Tsekouras, G.J.; Fopah-Lele, A. The Impact of Integrating Variable Renewable Energy Sources into Grid-Connected Power Systems: Challenges, Mitigation Strategies, and Prospects. *Energies* 2025, 18, 689. https://doi.org/10.3390/en18030689
8. Riurean, S.; Fîță, N.-D.; Păsculescu, D.; Slușariuc, R. Securing Photovoltaic Systems as Critical Infrastructure: A Multi-Layered Assessment of Risk, Safety, and Cybersecurity. *Sustainability* 2025, 17, 4397. https://doi.org/10.3390/su17104397
9. Yaacoub, J.P.A.; Noura, H.N.; Salman, O.; Chahine, K. Toward Secure Smart Grid Systems: Risks, Threats, Challenges, and Future Directions. *Future Internet* 2025, 17, 318. https://doi.org/10.3390/fi17070318
10. Moldovan, D.; Riurean, S. Cyber-Security Attacks, Prevention and Malware Detection Application, December 2022, Journal of Digital Science 4(2):3-19, DOI: 10.33847/2686-8296.4.2_1
11. Dorji, S.; Stonier, A.A.; Peter, G.; Kuppusamy, R.; Teekaraman, Y. An Extensive Critique on Smart Grid Technologies: Recent Advancements, Key Challenges, and Future Directions. *Technologies* 2023, 11, 81. https://doi.org/10.3390/technologies11030081
12. Boeding, M.; Scalise, P.; Hempel, M.; Sharif, H.; Lopez, J., Jr. Toward Wireless Smart Grid Communications: An Evaluation of Protocol Latencies in an Open-Source 5G Testbed. Energies 2024, 17, 373. https://doi.org/10.3390/en17020373
13. Riurean, S.M., Leba, M., Ionica, A.C. (2021). Conventional and Advanced Technologies for Wireless Transmission in Underground Mine. In: Application of Visible Light Wireless Communication in Underground Mine. Springer, Cham. https://doi.org/10.1007/978-3-030-61408-9_2
14. Ojo, K.E.; Saha, A.K.; Srivastava, V.M. Review of Advances in Renewable Energy-Based Microgrid Systems: Control Strategies, Emerging Trends, and Future Possibilities. *Energies* 2025, 18, 3704. https://doi.org/10.3390/en18143704
15. Chatuanramtharnghaka, B.; Deb, S.; Singh, K.R.; Ustun, T.S.; Kalam, A. Reviewing Demand Response for Energy Management with Consideration of Renewable Energy Sources and Electric Vehicles. *World Electr. Veh. J.* 2024, 15, 412. https://doi.org/10.3390/wevj15090412
16. Riurean, S., Rus, C. (2025). Optical Wireless Battery Management System for Enhanced Performance and Safety. In: Antipova, T. (eds) Digital Technology Platforms and Deployment. Information Systems Engineering and Management, vol 36. Springer, Cham. https://doi.org/10.1007/978-3-031-86547-3_23
17. Xu, N.; Tang, Z.; Si, C.; Bian, J.; Mu, C. A Review of Smart Grid Evolution and Reinforcement Learning: Applications, Challenges and Future Directions. Energies 2025, 18, 1837. https://doi.org/10.3390/en18071837
18. Kang, Y. Sustainable Development Through Energy Transition: The Role of Natural Resources and Gross Fixed Capital in China. *Sustainability* 2025, 17, 83. https://doi.org/10.3390/su17010083
19. Chrysikopoulos, S.K.; Chountalas, P.T.; Georgakellos, D.A.; Lagodimos, A.G. Decarbonization in the Oil and Gas Sector: The Role of Power Purchase Agreements and Renewable Energy Certificates. Sustainability 2024, 16, 6339. https://doi.org/10.3390/su16156339
20. Berrich, O. The Paris Agreement's Contribution to Renewable Energy Diffusion in Africa and Europe: A Panel Data Analysis. Energies 2024, 17, 4238. https://doi.org/10.3390/en17094238
21. Niște, D.-F.; Bobo, C.; Jilavu, A.; Badea, A.-F.; Bogdan, C. Electricity Losses in Focus: Detection and Reduction Strategies—State of the Art. *Applied Sciences* 2025, 15, 3517. https://doi.org/10.3390/app15073517
22. Luty, L.; Zioło, M.; Knapik, W.; Bąk, I.; Kukuła, K. Energy Security in Light of Sustainable Development Goals. Energies 2023, 16, 1390. https://doi.org/10.3390/en16031390
23. Wojtaszek, H. Energy Transition 2024–2025: New Demand Vectors, Technology Oversupply, and Shrinking Net-Zero 2050 Premium. *Energies* **2025**, *18*, 4441. https://doi.org/10.3390/en18164441
24. Li, M.; et al. Renewable energy quality trilemma and coincident wind–solar droughts. Communications Earth & Environment 2024. https://doi.org/10.1038/s43247-024-01850-5
25. Staadecker, M.; et al. The value of long-duration energy storage under various scenarios. Nature Communications 2024. https://doi.org/10.1038/s41467-024-53274-6
26. Rahman, M.M.; et al. An Overview of Power System Flexibility: High Renewable Energy Penetration. *Energies* 2024, 17, 6393. https://doi.org/10.3390/en17246393

 doi:10.20944/preprints202510.1006.v1

27. Monaco, R.; et al. Digitalization of power distribution grids: Barrier analysis, ranking and implications. *Energy Policy* 2024, 114083. https://doi.org/10.1016/j.enpol.2024.114083
28. Aghahadi, M.; et al. Digitalization Processes in Distribution Grids: A Comprehensive Review of Strategies and Challenges. *Applied Sciences* 2024, 14, 4528. https://doi.org/10.3390/app14114528
29. Ismail, F.B.; et al. A comprehensive review of the dynamic applications, benefits and impediments of digital-twin technology in the energy sector. *Sustainable Energy, Grids and Networks* 2024. https://doi.org/10.1016/j.segan.2024.101410
30. Jiang, H.; **et al.** A globally interconnected solar–wind system can meet future electricity demand. *Nature Communications* **2025**. https://doi.org/10.1038/s41467-025-59879-9
31. Adeyinka, A.M.; et al. Advancements in hybrid energy storage systems for grid-connected renewable integration: a review. *Sustainable Energy Research* 2024, 9, 1–27. https://doi.org/10.1186/s40807-024-00120-4
32. Naghibi, A.F.; et al. Capabilities of battery and compressed-air storage for flexibility regulation in multi-microgrids. Scientific Reports 2025, 15, 24856. https://doi.org/10.1038/s41598-025-06768-2
33. Štogl, O.; et al. Electric vehicles as facilitators of grid stability and flexibility: opportunities and challenges. WIREs Energy and Environment 2024, e536. https://doi.org/10.1002/wene.536
34. Gremes, M.F.; et al. NTL-Unet: A satellite-based approach for non-technical loss detection in electricity distribution using Sentinel-2 imagery and ML. *Sensors* 2024, 24, 4924. https://doi.org/10.3390/s24154924
35. Khalid, M.; Dabbaghjamanesh, M.; Goswami, S.; Arefifar, S.A. SG and Renewable Energy Systems: Perspectives and Grid Integration Challenges. Energy Strategy Reviews 2024, 51, 101299. https://doi.org/10.1016/j.esr.2024.101299
36. Athanasiadis, C.L.; Papadopoulos, T.A.; Kryonidis, G.C.; Doukas, D.I. A Review of Distribution Network Applications Based on Smart Meter Data Analytics. Renewable and Sustainable Energy Reviews 2024, 191, 114151. https://doi.org/10.1016/j.rser.2023.114151
37. Pourfarzin, S.; Ghafouri, M.; Askarzadeh, A. Technoeconomic Conservation Voltage Reduction–Based Demand Response for Distributed Power Networks. *International Transactions on Electrical Energy Systems* 2024, 2024, 9752955. https://doi.org/10.1155/2024/9752955
38. Cabot, P.; Girbau-Labagueria, J.; Olivella-Rosell, P.; Sumper, A. Demand-Side Flexibility in Liberalised Power Markets: From Technical Capabilities to Market Products and Standardised Services. Renewable and Sustainable Energy Reviews 2024, 187, 114694. https://doi.org/10.1016/j.rser.2023.114694
39. Hofmann, C.; Hirth, L.; Schlecht, I. Grid Tariff Design and Peak Demand Shaving: A Comparative Analysis between Germany and the United States. Energy Policy 2025, 192, 114777. https://doi.org/10.1016/j.enpol.2025.114777
40. Hua, L.; Wang, X.; Lin, H.; Wang, F.; Zhao, Y.; Zhang, T. Demand Response with Pricing Schemes and Consumers with Varying Preferences: A Comparative Analysis. Applied Energy 2025, 375, 123724. https://doi.org/10.1016/j.apenergy.2025.123724
41. Rouhani, Z.; Fereidunian, A.; Saderi, N. A Critical Review of Cybersecurity in Intelligent Renewable-Dominated Microgrids. Energy 2024, 293, 130409. https://doi.org/10.1016/j.energy.2024.130409
42. Paul, B.; Sarker, A.; Abhi, S.H. Potential Smart Grid Vulnerabilities to Cyber Attacks: Current Threats and Existing Mitigation Strategies. Heliyon 2024, 10, e37980. https://doi.org/10.1016/j.heliyon.2024.e37980
43. Liu, L.; Yuan, Y.; Wang, Z.; Yao, Y.; Ding, F. Integrated Framework of Multisource Data Fusion for Outage Location in Looped Distribution Systems. IEEE Transactions on Smart Grid 2025. https://doi.org/10.1109/TSG.2025.3540979
44. Silva, L.F.W.; Rodrigues, K.A.; Ribeiro, P.F.; Oleskovicz, M.; Kagan, N.; Chad, D.; Cardoso, da Silva, D.C.; et al. Islanding Detection Methods for Distributed Generation in Electric Power Systems: A Comprehensive Assessment. Scientific Reports 2024, 14, 16170. https://doi.org/10.1038/s41598-024-65573-9
45. Souza, M.A.; Gouveia, H.T.V.; Ferreira, A.A.; de Lima Neta, R.M.; et al. Detection of Non-Technical Losses on a Smart Distribution Grid Based on Artificial Intelligence Models. Energies 2024, 17, 1729. https://doi.org/10.3390/en17071729
46. Janev, V.; Berbakov, L.; Tomašević, N.; Sotoca, J.M.-B.; Lujan, S. Validating the Smart Grid Architecture Model for Sustainable Energy Community Implementation: Challenges, Solutions, and Lessons Learned. *Energies* **2025**, *18*, 641. https://doi.org/10.3390/en18030641

47. Basilico, P.; Biancardi, A.; D'Adamo, I.; Gastaldi, M.; Yigitcanlar, T. Renewable Energy Communities for Sustainable Cities: Economic Insights into Subsidies, Market Dynamics and Benefits Distribution. *Applied Energy* **2025**, *389*, 125752. https://doi.org/10.1016/j.apenergy.2025.125752
48. Official Journal of the European Union. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ%3AL_202401366 (accessed on 01.10.2025).
49. European Union Eur-Lex. Available online: https://eur-lex.europa.eu/eli/reg_del/2024/1366/oj/eng (accessed on 01.10.2025).
50. Federal Energy Regulatory Commission. Available online: https://www.ferc.gov/industries-data/electric/industry-activities/cyber-and-grid-security (accessed on 01.10.2025).
51. Ofgem. Available online: https://www.ofgem.gov.uk/energy-regulation/technology-and-innovation/cybersecurity. (accessed on 01.10.2025).
52. Australian Government Department of Home Affairs. Available online: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/slacip-bill-2022 (accessed on 01.10.2025).
53. Cybersecurity Agency of Singapore. Available online: https://www.csa.gov.sg/legislation/cybersecurity-act (accessed on 01.10.2025).
54. International Electrochemical Commission. Available online: https://webstore.iec.ch/en/publication/68410 (accessed on 01.10.2025).
55. ISO. Available online: https://www.iso.org/standard/85056.html (accessed on 01.10.2025).
56. IEEE Standard Association. Available online: https://standards.ieee.org/ieee/C37.118.1/4902
57. Electrifyng Europe. Available online: https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout. (accessed on 01.10.2025).
58. National Institute of Standards and Technology (NIST). Guidelines for Smart Grid Cybersecurity, NISTIR 7628, Rev. 1; NIST: Gaithersburg, MD, USA, 2014. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2014/nist.ir.7628r1.pdf (accessed on 25 September 2025).
59. International Electrotechnical Commission (IEC). IEC 62443 3 3:2013—System Security Requirements and Security Levels; IEC: Geneva, Switzerland, 2013. Available online: https://webstore.iec.ch/en/publication/7033 (accessed on 25 September 2025).
60. International Society of Automation (ISA). ISA/IEC 62443 Series of Standards—Overview. Available online: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (accessed on 25 September 2025).
61. North American Electric Reliability Corporation (NERC). CIP 002 5.1a—BES Cyber System Categorization; NERC: Atlanta, GA, USA, 2019. Available online: https://www.nerc.com/pa/stand/reliability%20standards/CIP-002-5.1a.pdf (accessed on 25 September 2025).
62. North American Electric Reliability Corporation (NERC). CIP 002 6—BES Cyber System Categorization; NERC: Atlanta, GA, USA, 2019. Available online: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-6.pdf (accessed on 25 September 2025).
63. North American Electric Reliability Corporation (NERC). CIP 013 2—Supply Chain Risk Management; NERC: Atlanta, GA, USA, 2022. Available online: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-2.pdf (accessed on 25 September 2025).
64. European Commission. Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration. Off. J. Eur. Union 2017, L 312, 54–93. Available online: https://eur-lex.europa.eu/eli/reg/2017/2196/oj/eng (accessed on 25 September 2025).
65. ENTSO E. Guidelines and Rules for Defence Plans in the Continental Europe Synchronous Area; ENTSO E: Brussels, Belgium, 2011. Available online: https://www.entsoe.eu/fileadmin/user_upload/_library/publications/entsoe/RG_SOC_CE/RG_CE_ENTSO-E_Defence_Plan_final_2011_public.pdf (accessed on 25 September 2025).
66. ENTSO E. System Defence Plan (v8, Draft); ENTSO E: Brussels, Belgium, 2022. Available online: https://www.entsoe.eu/Documents/SOC%20documents/Regional_Groups_Continental_Europe/2022/220215_RGCE_TOP_03.2_D.1_System%20Defence%20Plan_v8_final.pdf (accessed on 25 September 2025).

doi:10.20944/preprints202510.1006.v1

67. ENTSO E. Operation Handbook—Policy 5 (Emergency Operations); ENTSO E: Brussels, Belgium. Available online: https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/entsoe/Operation_Handbook/Policy_5_final.pdf (accessed on 25 September 2025).
68. National Institute of Standards and Technology (NIST). Cybersecurity Framework (CSF) 2.0; NIST: Gaithersburg, MD, USA, 2024. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (accessed on 25 September 2025).
69. National Institute of Standards and Technology (NIST). CSF 2.0 Resource & Overview Guide (SP 1299); NIST: Gaithersburg, MD, USA, 2024. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf (accessed on 25 September 2025).
70. Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic cascade of failures in interdependent networks. Nature 2010, 464, 1025–1028. https://doi.org/10.1038/nature08932.
71. Liu, Y.; Ning, P.; Reiter, M.K. False Data Injection Attacks against State Estimation in Electric Power Grids. In Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09), Chicago, IL, USA, 9–13 November 2009; pp. 21–32. Available online: https://reitermk.github.io/papers/2009/CCS1.pdf (accessed on 25 September 2025).
72. ENTSO E. Continental Europe Synchronous Area Separation on 08 January 2021—Final Report; ENTSO E: Brussels, Belgium, 2021. Available online: https://www.entsoe.eu/Documents/SOC%20documents/SOC%20Reports/Continental%20Europe%20Synchronous%20Area%20Separation%20on%2008%20January%202021%20-%20Main%20Report_updated.pdf (accessed on 25 September 2025).
73. ENTSO E. Executive Summary: Continental Europe Separation on 08 January 2021; ENTSO E: Brussels, Belgium, 2021. Available online: https://www.entsoe.eu/Documents/SOC%20documents/SOC%20Reports/Continental_Europe_Synchronous_Area_Separation_on_08_January_2021_-_Executive_Summary_updated.pdf (accessed on 25 September 2025).
74. Dan Codruț Petrilean, Nicolae Daniel Fîță, Gabriel Dragoș Vasilescu, Mila Ilieva-Obretenova, Dorin Tataru, Emanuel Alin Cruceru, Ciprian Ionuț Mateiu, Aurelian Nicola, Doru-Costin Darabont, Alin-Marian Cazac, Sustainability Management Through the Assessment of Instability and Insecurity Risk Scenarios in Romania's Energy Critical Infrastructures, MDPI – Multidisciplinary Digital Publishing Institute, Sustainability 17, no. 7: 2932, https://doi.org/10.3390/su17072932 (Q2), 2025.
75. Fita Nicolae Daniel, Ilie Utu, Marius Daniel Marcu, Dragos Pasculescu, Ilieva Obretenova Mila, Florin Gabriel Popescu, Teodora Lazar, Adrian Mihai Schiopu, Florin Muresan-Grecu, and Emanuel Alin Cruceru, Global Energy Crisis and the Risk of Blackout: Interdisciplinary Analysis and Perspectives on Energy Infrastructure and Security, MDPI – Multidisciplinary Digital Publishing Institute, Energies 18, no. 16: 4244. https://doi.org/10.3390/en18164244, 2025