Universal Library of Multidisciplinary | Methodological Guide

ISSN: 3064-9986 | Volume 2, Issue 2

Open Access | PP: 44-55

DOI: https://doi.org/10.70315/uloap.ulmdi.2025.0202006

Smart Adaptive Energy Optimization (SAEO): Methodological Foundations and Prospects for Application in Modern Energy Systems

Petro Bondar

Founder of Skitter Sp. z O.O. (Poland), Skitter USA LLC (USA), Miami, USA.

Abstract

Against the backdrop of the rapid growth of global electricity demand, exacerbated by climate change and accelerated electrification, the energy sector faces a dual challenge: ensuring reliability while simultaneously decarbonizing the system. The handbook systematizes the interdisciplinary foundations of smart adaptive energy optimization (SAEO) as a key approach and establishes an integrated conceptual framework for the design, deployment, and evaluation of SAEO systems. It is demonstrated that SAEO increases the stability of hybrid renewable energy systems, optimizes demand-side management, strengthens predictive maintenance, and improves techno-economic performance indicators. At the same time, barriers to scaling are identified: high computational costs, data infrastructure requirements, and new classes of systemic risks driven by the vulnerability of intelligent algorithms. A viable strategy for the transition to the next generation of intelligent, autonomous, and sustainable energy systems is a holistic, system-integrated approach that treats control, modeling, and security as an inseparable whole. The materials are intended for researchers, power engineers, system architects, and regulators.

Keywords: *Smart Adaptive Energy Optimization, Deep Reinforcement Learning, Digital Twins, Cybersecurity, Hybrid Renewable Energy Systems, Demand-Side Management.*

INTRODUCTION

The global energy system is undergoing a qualitative restructuring in which two powerful, at times conflicting impulses intersect: the accelerated build-up of electricity demand and the requirement for deep decarbonization as a key instrument for countering climate risks. The indicators for 2024 demonstrate the scale of the challenge: aggregate global energy consumption increased by 2.2%, outpacing the average growth rates of the previous decade [1]. The balance has shifted particularly sharply in the power sector: electricity demand grew by 4.3%—almost twice as fast as global GDP growth [2]. This trajectory is explained by the cumulative effect of widespread electrification of transport and heat supply, the intensification of energy use in industry, and the rapid growth of loads created by data centers and artificial intelligence systems; extreme weather conditions that drove record cooling demand also contributed [36, 37].

Against this backdrop, the deployment of low-carbon technologies has accelerated. In 2024 renewables accounted for 38% of the increase in global energy consumption, and the combined share of clean generation (renewables plus nuclear power) reached 40% of global electricity production for the first time [2]. Nevertheless, the expansion of renewables still lags behind the pace of demand growth, and the resulting gap is being filled by fossil fuels. As a result, a paradoxical situation is taking shape: despite record capital expenditures on the development of green energy—USD 2.1 trillion in 2024—global CO_2 emissions continue to rise [2].

The energy transition is thus entering a more complex phase — its honeymoon period is effectively ending. Annual investment growth has slowed from 24–29% previously to 11% in 2024 [6]. This is not about lowering targets but about encountering systemic limits: rising project costs, increasing technological complexity, and the emergence of physical bottlenecks [7]. The shortages are most acute in the supply chains of critical power equipment; for example, delivery times for power transformers have lengthened from 50 weeks in 2021 to 120–210 weeks in 2024 [9]. Consequently, the primary constraint on scaling renewables is not generation per se, but the throughput and readiness of grid infrastructure. Under these conditions, the emphasis must shift from merely adding capacity to the intelligent optimization of the entire energy system; this is why the

Citation: Petro Bondar, "Smart Adaptive Energy Optimization (SAEO): Methodological Foundations and Prospects for Application in Modern Energy Systems", Universal Library of Multidisciplinary, 2025; 2(2): 44-55. DOI: https://doi.org/10.70315/uloap.ulmdi.2025.0202006.

SAEO concept becomes not just important but critical for the successful implementation of the energy transition.

The academic corpus of existing research is saturated with works on energy system optimization. A wide spectrum of algorithms has been proposed — from classical analytical and stochastic schemes to sophisticated metaheuristics, including genetic algorithms (GA) and particle swarm optimization (PSO) [10]. However, a considerable share of this body of work addresses theoretical, static problem statements under idealizing assumptions. As a result, a gap persists between formal modeling and the construction of integrated, scalable, and secure frameworks suitable for operation in real, dynamically changing, and potentially adversarial cyber-physical environments [11].

Traditional optimization approaches generally do not provide the required adaptability for real-time control, especially under the high stochasticity characteristic of RES-based generation and modern consumption profiles [12]. In contrast, AI-oriented methods, despite demonstrated effectiveness, often operate as black boxes. Their deployment in critical infrastructure entails risks of unpredictable behavior and enlarges the attack surface, including false data injection attacks (FDIA) capable of poisoning model training [13]. Thus, the research gap lies in the absence of an integrated methodology that unifies three key aspects:

-intelligent control: Timely optimal decision-making under uncertainty;

-high-precision modeling: The availability of a validated digital (virtual) environment for safe testing and deployment of control algorithms;

-guaranteed security: Built-in mechanisms to counter cyber-physical threats targeting both the physical infrastructure and the control intelligence.

The goal is to systematize the interdisciplinary methodological foundations of SAEO and to propose an integrated conceptual framework for the design, deployment, and evaluation of such systems.

The scientific novelty lies in the formalization of a holistic SAEO architecture that synergistically integrates deep reinforcement learning agents (DRL) for adaptive action selection, digital twins (DT) as the operational simulation environment, and a multilayer cybersecurity paradigm as a necessary condition for resilience.

The author's hypothesis is based on the premise that achieving reliable, scalable, and secure autonomous optimization of energy consumption is determined not by perfecting any single technology but by the systemic integration of DRL, DT, and cybersecurity. Such synergy is the most realistic path to bridging the gap between theoretical constructs and practically viable, fault-tolerant SAEO systems.

CHAPTER 1. TECHNOLOGICAL AND THEORETICAL BASIS OF SAEO

Fundamental Principles of System Optimization in the Energy Sector

At the core of any SAEO system lies a multiobjective optimization formulation aimed at finding a rigorously justified compromise among competing technical and economic performance indicators. Formally, the problem reduces to selecting a control strategy from an admissible set defined by hard constraints, while ensuring optimality in the sense of the chosen criterion approach (a vector criterion or its scalarization), that is, to the minimization or maximization of the corresponding objective function subject to all constraints.

The first priority is the minimization of total costs, typically through reducing the net present cost (NPC), the levelized cost of energy (LCOE), and/or operating expenditures (OPEX), including the fuel component and maintenance costs [16]. This approach ensures intertemporal comparability of alternatives and allows accounting for both capital and operational effects.

The second priority is the minimization of greenhouse gas emissions, that is, the deliberate reduction of the energy system's carbon footprint measured in tonnes of CO_2 equivalent. This criterion integrates environmental requirements into the optimization procedure and serves as a tool for aligning energy and climate objectives [17].

The third priority is the maximization of reliability, understood as ensuring continuity of energy supply given the demand structure and resource constraints. In practice, this is expressed either by minimizing the Loss of Power Supply Probability (LPSP) or by maximizing the integral reliability index (Reliability, REL), which makes it possible to quantitatively rank solutions by their resilience to failures and variability of operating regimes [10].

Optimization of operating modes and dispatch control of the power system are carried out under strict system-level constraints determined by both fundamental physical laws and operational regulations. At every moment it is necessary to ensure the balance of active power: the aggregate generation output must strictly match the total demand with account for network losses. It is no less important to maintain power quality indicators — voltage and frequency — within standardized ranges that guarantee stability and safe operation of equipment. Additionally, operational limits of infrastructure elements — generators, storage units, and network devices — must be observed: ranges of minimum and maximum active/reactive power, permissible ramp-up and ramp-down rates, and for battery systems — requirements for state of charge (SoC) and associated technological constraints [10, 31].

Historically, analytical and probabilistic approaches, as well as metaheuristics (for example, particle swarm optimization, PSO, and genetic algorithms, GA) [10], have been used to solve such problems. However, in high-dimensional, dynamic, and stochastic formulations characteristic of modern power systems, their effectiveness decreases substantially: the search for quasi-global extrema leads to a rapid growth of computational costs, high sensitivity to disturbances makes the obtained solutions unstable, and the transferability of tuning across operating modes remains limited. As a result, the listed methods prove to be of little use for real-time operational control, where predictability of computations, strict satisfaction of intricately coupled constraints, and guarantees of safe operation are critical.

Architecture of Intelligent Agents Based on Deep Reinforcement Learning (DRL)

Deep reinforcement learning (DRL) is a machine learning paradigm aimed at constructing intelligent agents that learn optimal strategies through repeated interaction with the environment. This approach naturally corresponds to the tasks of controlling complex dynamic systems, among which are modern electric power systems with their pronounced nonlinearities, stochasticity, and stringent operational constraints.

In the context of power system control, the basic elements of the DRL framework are defined as follows [12]. An agent is a control program, typically implemented on a neural network architecture and making decisions at discrete time instants. In SAEO systems this is effectively a controller that sets the operating modes of generators, storage units, and controllable loads. The environment is the physical power system or its high-fidelity digital twin, from which the agent receives responses to its actions.

The state of the environment is interpreted as an informative feature vector describing the operation of the system at time t. It may include nodal load levels, instantaneous values of RES generation, market electricity prices, the state of charge of batteries, and other technological parameters sufficient for making correct decisions under partial observability and process stochasticity.

An action is a control input formed by the agent based on the observed state. Typical examples include changing a generator's active power by ΔP, setting the storage charging current I, or initiating the disconnection of a specific group of consumers within demand response programs; both discrete and continuous action spaces are admissible, which predetermines the choice of algorithmic technique.

Reward represents a numerical feedback signal returned by the environment after an action is applied. The reward function is designed so that its maximization is aligned with the operator's objectives: minimizing total costs, complying with technical and market constraints, improving reliability and stability of operation; positive incentives are set, for example, for cost reduction, while penalties are imposed for constraint violations, deviations of power quality parameters, and unserved energy [12].

Compared to traditional control methods, the advantages of DRL are significant [12]. First, adaptive learning is ensured: the agent continuously refines its strategy as external conditions change, whereas the rule-based logic of classical controllers is static. Second, high autonomy is achieved: nontrivial policies are discovered without their explicit encoding by a human. Third, the algorithms scale to high-dimensional state and action spaces, where classical approaches (for example, dynamic programming) face the curse of dimensionality. Finally, DRL is robust to incomplete and noisy data, which is critical for real power systems with limited observability.

The choice of a particular algorithm is determined by the nature of the task (discrete or continuous), the requirements for training stability, data efficiency, and the acceptable variability of policies. In practice, methods are used that can handle continuous actions and ensure stable convergence under limited interaction trajectories with the environment, which is especially important when training on a digital twin and subsequently transferring the policy to real-world operation (see Table 1).

Table 1. Comparison of key DRL algorithms for application in intelligent energy systems (compiled by the author based on [12, 25, 33]).

Algorithm	Type	Action space	Key advantages	Typical applications
Deep Q-Network (DQN)	Value-based (Value-based)	Discrete	High data efficiency, relative simplicity of implementation.	Electric vehicle charging control (on/off), switching equipment operating modes.
Proximal Policy Optimization (PPO)	Policy-based (Policy-based)	Discrete/ Continuous	High training stability and reliability, good balance between efficiency and complexity.	Smooth power control of energy storage systems, generation regulation, participation in ancillary services markets.
Advantage Actor-Critic (A2C/A3C)	Actor-Critic (Actor-Critic)	Discrete/ Continuous	Ability for parallel training (A3C), which speeds up the process.	Comprehensive microgrid control, coordination of distributed energy resources.

In general, the architecture of DRL-based intelligent agents naturally aligns with the control tasks of modern electric power systems: the agent (a neural network controller), interacting with a digital twin or a real grid, at each step forms an action based on the observed state and receives a reward whose objective function is aligned with operational priorities (minimization of costs, compliance with technical and market constraints, reliability and stability). This formulation provides key advantages over classical methods: adaptability to nonlinearity and stochasticity, autonomous discovery of nontrivial strategies, scalability to high dimensionalities, and robustness to noise/incomplete observability. The choice of algorithm is dictated by the nature of control and the requirements for training stability and efficiency, as well as for the transferability of the policy from the digital twin to the real control loop: DQN is appropriate for discrete actions (e.g., switching/on-off), PPO — for continuous control with heightened stability requirements (smooth regulation of storage, generation, system reliability services), A2C/A3C — when parallel training and coordination of distributed resources are needed. Consequently, the correct formalization of states/actions/rewards and a deliberate choice of DRL method make it possible to build autonomous controllers capable of safely and economically operating complex power systems under uncertainty.

The Concept of Digital Twins (Digital Twins) as an Operational Environment for SAEO

The application of deep reinforcement learning in critical energy infrastructure encounters a fundamental obstacle: a learn-by-failure strategy is unacceptable, since even a single control error in a real power system can trigger cascading outages, damage expensive equipment, and generate systemic risks for the reliability of energy supply [13]. A digital twin (DT) resolves this contradiction by providing a physically consistent, high-accuracy, and safe virtual environment suitable for the training, testing, and verification of DRL agents.

In the power sector, a DT is interpreted not as a static simulation scheme, but as a dynamic virtual replica of the physical power system, maintained in a near real-time mode and linked to it by bidirectional data flows [19]. The typical architecture of such a solution includes three mutually complementary layers [21]: the physical layer, covering generators, transmission lines, substations, consumers, sensors, and actuators; the virtual layer, containing mathematical models of components and processes that ensure their high-accuracy behavioral reproduction; the data and communication layer, integrating sensing, communication networks (including 5G), and industry protocols such as IEC 61850, for synchronizing measurements and transmitting control actions between the physical and virtual sides.

Owing to this organization, a DT ceases to be merely a simulator and becomes an infrastructural instrument that makes the application of artificial intelligence methods in a critical environment practice-oriented and safe. In essence, a DT serves as a bridge from theory to operations: it enables transferring algorithms from the laboratory to the real power system while minimizing technological and operational risks [19].

The conceptual architecture of the proposed system, illustrating the interrelation of its key components, is presented in Figure 1.

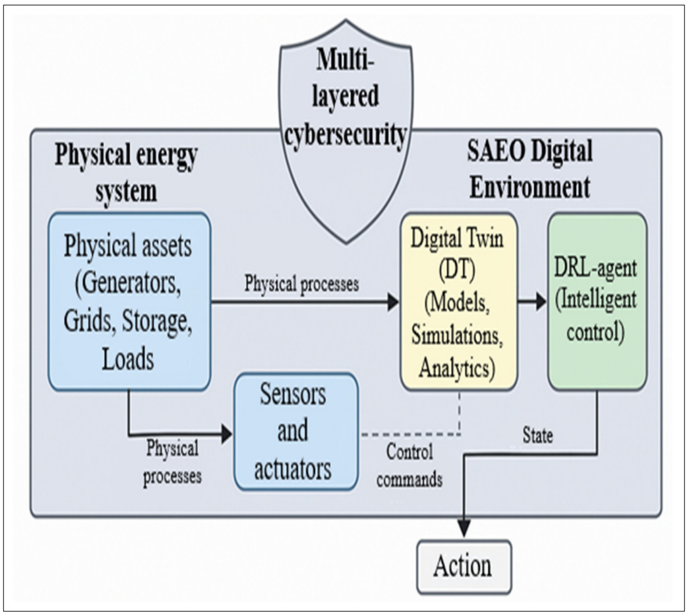

Figure 1. Conceptual architecture of the integrated SAEO system (compiled by the author based on [13, 19, 29, 32]).

Within SAEO, the key functions of the DT form an end-to-end cycle for the development and deployment of intelligent control. First, the DT serves as a training environment for DRL agents: millions of iterations can be executed in accelerated time without any impact on the physical system and without associated risks [13, 19]. Second, verification and validation are ensured: before operational deployment, any new control strategy is tested across thousands of scenarios, including rare and extreme modes, which increases confidence in the algorithms and reduces the likelihood of undesirable states when inserted into the real control loop [19].

Third, the DT supports predictive modeling: accurate forecasts of renewable generation and load levels provide the agent with high-quality input data, increasing the robustness and optimality of the resulting decisions [19]. Fourth, continuous asset condition monitoring and predictive maintenance rely on State of Health (SoH) assessment and Remaining Useful Life (RUL) forecasting; this enables the SAEO system to adaptively select operating modes, extending equipment service life and reducing total life-cycle costs [19, 30].

Finally, the DT provides a controlled platform for failure analysis and cyberattack modeling: in a safe environment it is possible to reproduce complex emergency scenarios, investigate vulnerabilities, and verify mechanisms of fault tolerance and self-healing without risk to the real power system. Taken together, these capabilities form an integrated loop for the development, testing, and reliable deployment of intelligent control methods in the electric power industry.

Cyber-Physical Security of SAEO Systems

The infusion of information and control technologies into the physical energy domain radically redefines it as a cyber-physical system (Cyber-Physical System, CPS) — a tightly coupled network of sensing, computing nodes, and actuators [13]. The optimization effect under such coupling is colossal, but the expansion of the digital surface inevitably generates new classes of vulnerabilities. In this configuration, SAEO effectively serves as the brain center of the CPS and therefore becomes a primary target of attacks. Hence follows a methodological imperative: cybersecurity cannot be considered an external superstructure; it must be constitutively embedded in the SAEO architecture and function as its immune system.

The threat landscape for SAEO is multidimensional and dynamic [14]. Availability attacks (DoS) include deliberate overloading of communication channels and computing resources, leading to degradation or shutdown of control loops. In distributed power systems that are sensitive to delays and packet losses, such impacts directly undermine the stability of operating modes and complicate safe recovery after disturbances.

The most destructive are attacks on data integrity (FDIA), because they erode trust in measurements that underlie state estimation and decision making. The injection of statistically plausible distortions can not only deceive the state estimation module but also poison the training of a DRL agent, shifting its policy toward suboptimal or risky strategies [14]. The systemic consequences are manifested in covert destabilization of operating modes and the accumulation of risks that are not detected by standard consistency tests.

No less significant is the privacy measurement vector. Passive interception of telemetry and consumption profiles reveals commercially sensitive information and aspects of users private lives, creating a basis both for targeted attacks and for unscrupulous handling of data [14].

A substantial share of the aggregate risk is formed by malware and supply chain attacks: the insertion of modified code into the software stacks of controllers and digital twins (DT) at the stages of manufacturing, updating, and maintenance. This picture is complemented by advanced persistent threats (APT) — multistage, latent campaigns aimed at the long-term seizure of control over SCADA and associated subsystems [14, 27].

In such an adversarial environment, only defense-in-depth remains viable — a coordinated composition of technical, organizational, and regulatory measures with overlapping areas of responsibility and mutual redundancy of detection, containment, and recovery functions [15, 18]. End-to-end alignment of access, monitoring, and response policies at all levels — from the edge to decision-making centers — is critical.

Technical countermeasures should start with strict network segmentation and perimeter control: specialized firewalls and intrusion detection/prevention systems (IDS/IPS), adapted to the semantics of industrial protocols and the topology of power networks, provide baseline isolation of critical control loops and early indication of anomalies [14, 20]. They are reinforced by allowlisting mechanisms, microsegmentation, and a strict principle of least privilege.

Cryptographic protection is the default norm: end-to-end encryption, strong authentication, key management, and integrity control must cover all channels and data both in flight and at rest, providing cryptographically verifiable immutability and authenticity of telemetry and commands [22, 23]. Practical implementation must account for stringent latency constraints and real-time computational budgets.

A promising direction is AI-based anomaly detection: machine learning models trained on multi-domain features (measurement streams, network metadata, event logs) detect deviations characteristic of stealthy FDIA and composite attacks, increasing sensitivity at an acceptable false alarm level [21]. It is essential to ensure their adversarial robustness and to validate them on representative real-world data.

The security of the digital twin and the DRL agent requires regular verification and validation cycles, the use of sandboxes for safe shakedown testing of updates, as well as continuous integrity monitoring of data, model weights, and training artifacts. MLOps pipelines should include verifiable provenance chains (provenance), strict versioning, and rollback policies that minimize the risk of unnoticed compromise.

Finally, blockchain is considered a mechanism for ensuring immutability and transparency of transactions and logs in decentralized energy architectures. When properly integrated, the distributed ledger increases trust in auditing and reconciliation of accounting events; however, its deployment must be aligned with the throughput and latency requirements of critical operations [14]. Taken together, the listed measures form a coherent defense system, where each layer reinforces the others, and the full configuration — from cryptography to AI detectors — provides the required cyber resilience of SAEO within CPS [15], [21, 23]. Below, Table 2 describes the Threat–Countermeasure matrix for the key components of the SAEO system [13, 15, 21, 23].

Table 2. Threat–Countermeasure Matrix for key components of the SAEO system (compiled by the author based on [13, 15, 21, 23]).

Component / Threat	False Data Injection (FDIA)	Denial of Service (DoS)	Data interception	Malware
Sensors and field devices	State estimation with bad data detection (BDD); sensor redundancy.	Physical protection; network segmentation.	Encryption of the communication channel (e.g., TLS/IPsec).	Firmware integrity verification; secure boot.
Communication network	Message authentication (e.g.,HMAC);cryptographic protocols.	Intrusion prevention systems (IPS); traffic filtering.	End-to-end encryption; virtual private networks (VPN).	Deep packet inspection (DPI); network antivirus.
Digital twin database	Data integrity control; blockchain for transaction logs.	Data backup and replication; load balancing.	Data-at-rest encryption; strict access control.	Malware scanning; access control.
DRL agent (control model)	Robust training methods; anomaly detectors on input data.	Isolation of the computing environment; rate limiting.	Protection against model extraction (Model Extraction).	Model verification; execution in an isolated environment (sandbox).

That is, the cyber-physical nature of SAEO makes it simultaneously the center of the power system and a primary target, so security must be built into the architecture from the outset as an immune function rather than a bolt-on. The diversity of threats — from DoS and privacy leaks to FDIA, APT, and supply-chain compromise — requires multilayered defense with overlapping areas of responsibility: strict segmentation and the principle of least privilege, industry-grade IDS/IPS and DPI, end-to-end cryptography under hard latency constraints, as well as AI-based anomaly detectors with verified adversarial robustness. The digital twin and the DRL agent must be accompanied by mature MLOps practices (verifiable provenance of data and weights, versioning, rollbacks, sandboxes, and continuous integrity monitoring), and distributed ledgers should be applied selectively for immutable accounting and audit where throughput and latency permit. Taken together, the systemic alignment of technical, organizational, and regulatory measures across the entire vertical — from the edge to the decision-making centers — forms resilient defense that reduces the risk of covert destabilization of operating regimes, protects privacy, and ensures the required cyber-resilience of SAEO within the CPS.

CHAPTER 2. APPLIED ASPECTS, BARRIERS, AND PROSPECTS OF SAEO

Optimal Control of Hybrid Renewable Energy Systems (HRES)

Hybrid renewable energy systems (HRES), combining stochastic generation sources (photovoltaic panels, wind turbines), a gas–steam turbine, and energy storage systems (ESS), constitute a representative testbed for applying SAEO. In this configuration, all primary energy sources — solar panels, the wind turbine, and the gas–steam turbine — interact as a single organism under SAEO. Diesel generators do not participate in normal load sharing and are engaged solely as emergency protection in the event of complete failure of all other system components. The control complexity here arises from the real-time requirement to reconcile intermittent RES-based generation with demand dynamics while simultaneously making economically optimal decisions regarding the engagement of storage and the main generating capacity [26].

Application of the SAEO framework provides a highly effective solution to this problem. A DRL agent trained in an HRES digital twin environment derives a complex nonlinear dispatch policy (dispatch strategy). It acts not reactively but proactively: it charges the ESS in advance using daytime solar generation to cover the evening demand peak or smoothly brings the gas–steam turbine to an economically optimal operating mode, thereby reducing fuel consumption and equipment wear. An illustrative example of the advantages of SAEO in energy storage control is shown in Figure 2.

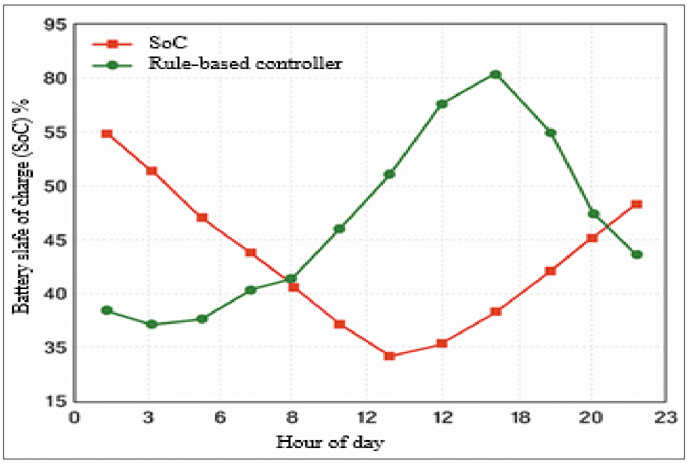

Figure 2. Simulation of the state of charge (SoC) management of the SNE (compiled by the author based on [1-5; 34, 35]).

As a result, a compromise that is difficult to achieve for rigidly regulated controllers is attained between the levelized cost of energy (LCOE) and the reliability index of power supply

(LPSP). The outcome of such optimization is a more favorable trade-off between cost and reliability, as illustrated by the Pareto front in Figure 3.

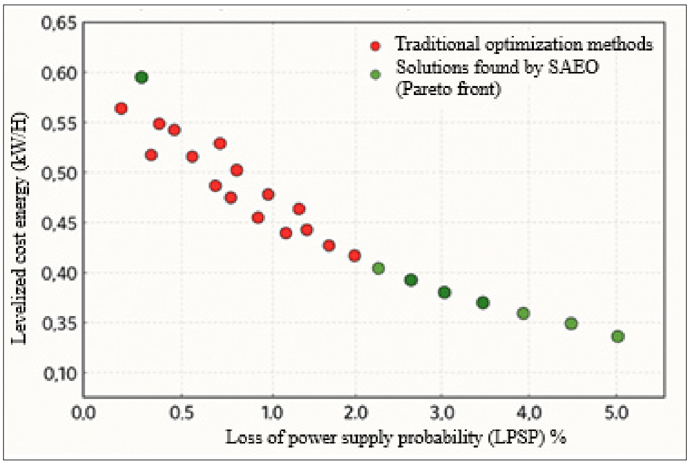

Figure 3. Optimizing the trade-off between cost and reliability of HRES (compiled by the author based on [6-9]).

Thus, it can be stated that the application of SAEO in hybrid energy systems based on renewable sources — with photovoltaic and wind installations, a gas–steam turbine, and energy storage — ensures practically realizable optimal real-time control under conditions of stochastic generation and dynamic demand. Diesel generators in this case perform exclusively the function of emergency protection. A DRL agent trained in a digital twin environment establishes a proactive nonlinear dispatch strategy that charges the storage in advance with daytime solar energy to cover evening peaks and, when necessary, brings the gas–steam turbine to its economically optimal operating mode, reducing fuel consumption and equipment wear. The SoC control results (Fig. 2) demonstrate the attainment of a compromise between LCOE and LPSP that is difficult for rigid controllers, and the resulting Pareto front (Fig. 3) shifts toward lower costs at a given reliability (or higher reliability at fixed costs), which confirms the effectiveness of SAEO for joint optimization of the economic performance and reliability of HRES.

Adaptive Demand Response (Demand Response) and Predictive Maintenance

The capabilities of SAEO extend substantially beyond simple generation dispatch. Two central application areas are adaptive demand response (DR) and predictive maintenance.

Adaptive Demand Response: classical DR programs that rely on fixed tariff grids (for example, day–night) demonstrate limited effectiveness. SAEO shifts control to a mode of fully dynamic and personalized coordination. A DRL agent, trained on large volumes of smart-meter data within the digital twin (DT) loop, extracts complex behavioral consumption patterns and derives proactive policies. Instead of coarse price signals, SAEO generates targeted incentives, promptly modifies tariffs in real time, and coordinates groups of devices (air conditioners, water heaters, electric vehicle charging stations) for fine shaping of the load curve, which provides peak shaving, reduction of aggregate costs, and increased grid resilience [28].

Predictive Maintenance: the inclusion of asset state-of-health (SoH) indicators in the SAEO loop adds a new dimension to optimization. The digital twin continuously monitors key equipment operating parameters (for example, transformer winding temperature, turbine bearing vibration), and the resulting features are supplied to the DRL agent as components of the state vector. As a result, the agent optimizes operating regimes not only in terms of short-term economic efficiency but also with regard to long-term wear. It can, for example, slightly offload an overheating transformer or choose an ESS operating profile that minimizes cell degradation, thereby extending the lifetime of costly assets and reducing total life-cycle costs [19].

Techno-Economic Analysis and Scaling of SAEO Solutions

Despite evident technological maturity, the diffusion of SAEO solutions encounters a combination of techno-economic and organizational barriers that objectively constrain the pace and amplitude of diffusion of the corresponding practices.

First, the configuration of costs is the key limiter. The deployment of SAEO is characterized by high capital intensity (CAPEX): it requires building a computational stack for digital twins (DT) and deep reinforcement learning (DRL) algorithms — from high-performance servers to cloud platforms; pervasive instrumentation of energy assets with sensors and IoT devices; as well as modernization of the communications infrastructure for reliable real-time data transmission. Operating expenditures (OPEX) are driven by software licensing, large-scale data management, and ensuring cyber-resilience, as well as the scarce competencies of interdisciplinary teams at the intersection of power engineering, data science, and information security [9].

Second, substantial technological challenges persist. Scaling DT architectures from the level of an individual microgrid to a regional or national power system generates extremely high computational loads; at the same time, the robust maintenance of synchronization and coherence of a multi-module model in real time remains an open research problem that requires new approaches to distributed computing and model verification [21].

Third, the existing economic and market institutions are poorly adapted to the specifics of SAEO. The established formats for organizing wholesale and retail electricity markets, as well as tariff regulation, often fail to ensure reliable monetization of the effects created—enhanced flexibility, reduced system costs, and the provision of system services. The absence of a transparent business case and long-term investment signals, including predictable returns on the corresponding services, complicates investment decision-making and the scaling of pilot projects [24, 26].

Finally, infrastructural constraints exert a critical impact. Physical infrastructure often becomes a bottleneck: long lead times for high-tech components, as well as complex and protracted procedures for approvals and permits for the construction of new transmission lines, offset the benefits of intelligent control, prolonging implementation timelines and increasing the total cost of projects [9]. Table 3 presents an analysis of techno-economic barriers to the deployment of SAEO.

Table 3. Analysis of techno-economic barriers during SAEO deployment (compiled by the author based on [7, 9, 21, 24, 26]).

Barrier type	Specific problem	Possible mitigation strategy
Technical	High computational costs for DT and DRL.	Use hybrid cloud/edge computing (Cloud/Edge Computing); development of reduced-order models.
Technical	DT scalability problem.	Modular, federated approach to building DT; standardization of data exchange interfaces.
Economic	High upfront capital expenditures (CAPEX).	Phased implementation starting with pilot projects at critical facilities; infrastructure as a service (IaaS) models.
Economic	Absence of market mechanisms for monetizing flexibility.	Electricity market reform; introduction of charges for ancillary services; development of new tariff structures.
Regulatory	Outdated regulations and standards.	Development of new technical regulations and standards for intelligent control systems; creation of regulatory sandboxes.
Regulatory	Data ownership and privacy issues.	Clear legal definition of data rights; implementation of privacy-preserving technologies (for example, homomorphic encryption).
Personnel	Shortage of specialists with interdisciplinary competencies.	Targeted educational programs at universities; corporate training centers; partnerships with IT companies.

Overall, the techno-economic analysis shows that the scaling-up of SAEO is constrained by a combination of factors: high capital intensity (construction of the DT/DRL stack, sensors/IoT, communications) and substantial OPEX (licenses, data management, cyber-resilience, workforce shortages); unresolved technological challenges (extreme computational loads and maintaining real-time synchronization of multi-module DTs); institutional market unpreparedness (weak monetization of flexibility and system services, lack of predictable investment signals); as well as infrastructural bottlenecks (long lead times for supply and permitting procedures). To overcome the barriers, an integrated program is required: technically — hybrid cloud/edge architectures, reduced-order models, modular-federated DTs with standardized data exchange interfaces; economically — phased pilots at critical facilities, IaaS approaches and market reforms with remuneration for ancillary services and adaptive tariffs; regulatory — updates of standards and regulatory sandboxes, legal certainty of data rights and the deployment of privacy-preserving technologies (including homomorphic encryption); organizationally — targeted training programs and partnerships with IT companies. Systematic execution of these steps, with a focus on TCO and cyber-resilience, will enable the deployment of scalable business cases and accelerate the diffusion of SAEO.

Risks, limitations, and Future Research Directions

The transition to AI-based autonomized control of power systems not only removes a layer of legacy problems but also creates fundamentally new classes of systemic risks. The same intelligent component that makes SAEO a highly effective instrument simultaneously makes it a target for intelligent and adaptive attacks. As a result, risk scenarios shift from failures of individual physical nodes (for example, transformer outages) to algorithmically induced systemic failures capable of evolving in a cascading manner and exceeding customary operational assumptions. This shift dictates an interdisciplinary research agenda at the intersection of power engineering, computer science, control theory, and cybersecurity.

A key source of vulnerabilities is the brittleness and limited capacity of models to generalize. DRL approaches that rely on historical data and synthetic scenarios often exhibit inadequate—and at times dangerous—behavior when confronted with black swans: rare, previously unobserved regimes absent from the training corpus. Sensitivity to distribution shifts and to incomplete descriptions of the environment increases the likelihood of erroneous control policies precisely during periods when maximal robustness and predictability are required.

No less significant is the black box of decision making. The opacity of deep neural networks complicates error attribution, undermines institutional trust, and complicates the certification of autonomous solutions for critical infrastructure [15, 25]. The deficit of interpretability blocks the deployment of formal verification procedures and accountability mechanisms necessary for regulatory compliance. To summarize strengths and weaknesses, as well as opportunities and threats associated with the adoption of SAEO, a SWOT analysis was conducted, the results of which are presented in Figure 4.

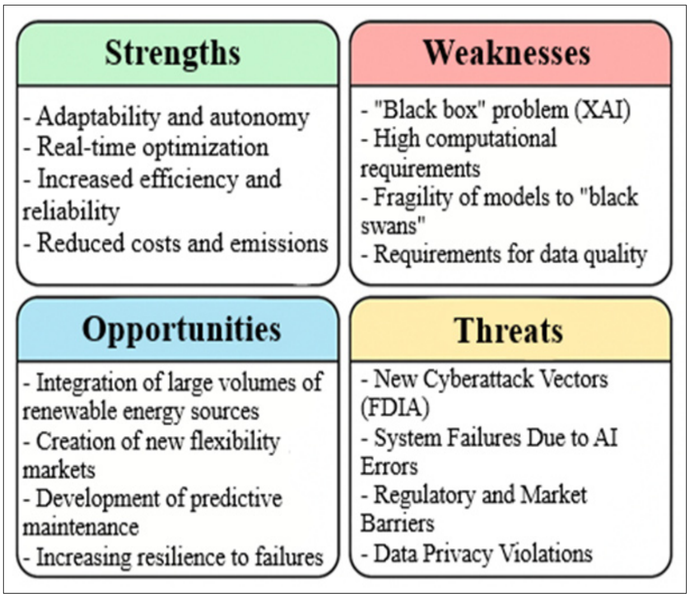

Figure 4. SWOT analysis of the SAEO paradigm.

An additional layer of risk is associated with data privacy and security. SAEO operates large-scale, highly granular streams of measurements and commercially sensitive information, which heightens the challenges of protecting personal data and safeguarding trade secrets, including threats of unauthorized access, leaks, and delayed attacks via the compromise of training datasets [22, 23]. The deployment of SAEO is not only a contribution to resilience and climate stability but also a driver of economic growth. It is a system in which every unit of capital invested yields a return in the form of savings, jobs, investment, and geopolitical influence.

The deployment of the SAEO system is not an isolated IT initiative but a profound restructuring of the production–energy system, generating substantial macroeconomic and climate outcomes. The impact is multilevel: from households and municipalities to the corporate sector and federal public finances, covering a wide range of industries from high technology to the agricultural sector.

The basic direct effect is expressed in a reduction of the aggregate cost of energy supply. Decentralization of generation reduces network losses and increases infrastructure resilience; the use of mechanisms for utilization of surplus output and peak shaving reduces the need for costly reserve capacity; the implementation of artificial intelligence systems increases the accuracy of demand forecasting and optimizes operating modes, thereby reducing operating costs; the substitution of imported energy carriers with locally produced hydrogen and renewable energy reduces currency risks. Taken together, this can provide savings on the order of 100–150 billion US dollars per year at the national level.

The consolidated socio-economic effect manifests through strengthening employment and accelerating technological renewal. The growth of manufacturing and service support for renewable energy equipment, the construction and operation of hydrogen infrastructure, and the development of AI models and digital energy management platforms create stable demand for engineering and IT competencies. Agriculture fits organically into this framework: decentralized microgrids based on biogas and hydrogen increase the energy autonomy of agricultural enterprises. The potential increase in employment is estimated at up to 2 million jobs in the United States by 2040.

The investment impulse of SAEO is expressed by an inflow of private capital into generating capacities, storage systems, and distributed microgrids, simultaneously increasing the investment attractiveness of regions. Energy independence stimulates the economic development of remote territories and lowers infrastructure barriers for small and medium-sized businesses; access to clean energy is capitalized in the value of real estate and industrial sites. The cumulative volume of private investment may reach around 500 billion USD over a 10–15-year horizon.

The fiscal result is also important. The reduction of subsidies for fossil fuels and the decrease in medical expenditures due to cleaner air are combined with lower costs for eliminating the consequences of climate-induced disasters. Additional savings arise from increased energy efficiency of military infrastructure facilities during the transition to SAEO microgrids. In total, this provides about 50–70 billion USD annually at the federal level.

Data management under such conditions should be regarded as a component of reliability architecture rather than an auxiliary function. Promising research directions aim to overcome the stated limitations. First, explainable AI (explainable AI, XAI) methods are required that provide interpretability of DRL agents decisions and traceability of their logic in terms relevant to engineering practice and regulatory oversight. These methods must be embedded directly into decision-making loops rather than applied exclusively post hoc.

Second, it is necessary to advance robust and transferable reinforcement learning: algorithms resilient to input data anomalies, distribution shifts, and partial observability, as well as mechanisms for rapid fine-tuning and adaptation to previously unseen conditions with strict safety guarantees.

Third, federated learning and privacy-preserving technologies constitute an important direction. Architectures that allow training on distributed datasets without their centralization make it possible to meet requirements for protecting personal and commercially sensitive data while maintaining model quality and timeliness.

Finally, software-hardware testbeds for verification (hardware-in-the-loop, HIL) are required, in which the DRL agent and the digital twin (digital twin, DT) interact with real equipment. Such testbeds provide testing conditions as close as possible to operation, reveal hidden interdisciplinary effects, and establish reproducible protocols for assessing reliability and safety prior to deployment in the network.

CONCLUSION

Within this study, a comprehensive analysis of the foundations of intelligent adaptive optimization of energy consumption (SAEO) was conducted. Comparison of current data for 2024 revealed systemic constraints of the energy transition: the outpacing growth of electricity demand and the hard physical limits of infrastructure. Under these conditions, shifting the emphasis from extensive capacity expansion to intensive, intelligently managed operation of the entire energy system becomes not merely preferable but the only viable option.

It has been demonstrated that a viable SAEO platform fundamentally cannot rely on a single technology line. The author's hypothesis of the need for synergistic integration of deep reinforcement learning (DRL), digital twins (DT), and multi-level cybersecurity is confirmed: DRL performs the functions of an adaptive brain, DT plays the role of an operational-simulation nervous system, and cybersecurity serves as the basic immune system ensuring the resilience of the entire cyber-physical organism.

The practical value of the work lies in forming a holistic perspective for three key groups of stakeholders. For engineers and system architects, a structured methodology for designing next-generation SAEO systems is presented. For the scientific community, the most pressing and critically significant trajectories for further research are outlined, including explainable AI, robust learning, and the protection of data privacy. For legislators and policymakers, the need for new market designs and regulatory frameworks is emphasized, stimulating the deployment of intelligent technologies and properly rewarding their contribution to enhancing the flexibility and reliability of energy systems.

Looking ahead, as current barriers are removed, energy systems will evolve toward fully autonomous, self-healing, market-oriented intelligent ecosystems. The SAEO paradigm presented in the study serves as the methodological core, a kind of operating system of this future, where energy management is carried out not merely efficiently but truly intelligently.

REFERENCES

1. Global trends [Electronic resource]. - Access mode: https://www.iea.org/reports/global-energy-review-2025/global-trends (date of access: 05.08.2025).
2. Global Energy Review 2025 [Electronic resource]. - Access mode:https://iea.blob.core.windows.net/assets/5b169aa1-bc88-4c96-b828-aaa50406ba80/GlobalEnergyReview2025.pdf (date of access: 05.08.2025).
3. Global Energy Review 2025 - Power Library [Electronic resource]. - Access mode: https://powerlibrary.theelectricityhub.com/2025/03/24/global-energy-review-2025/ (date of access: 05.08.2025).
4. Global Energy Review 2025 – Analysis - IEA [Electronic resource]. - Access mode: https://www.iea.org/reports/global-energy-review-2025 (date of access: 07.08.2025).
5. Global Electricity Review 2025 - Ember [Electronic resource]. - Access mode: https://ember-energy.org/app/uploads/2025/04/Report-Global-Electricity-Review-2025.pdf (date of access: 07.08.2025).
6. Global Investment in the Energy Transition Exceeded $2 Trillion for the First Time in 2024, According to BloombergNEF Report [Electronic resource]. - Access mode: https://about.bnef.com/insights/finance/global-investment-in-the-energy-transition-exceeded-2-trillion-for-the-first-time-in-2024-according-to-bloombergnef-report/ (date of access: 07.08.2025).
7. Global Energy Perspective 2024 - McKinsey [Electronic resource]. - Access mode: https://www.mckinsey.com/~/media/mckinsey/industries/energy%20and%20materials/our%20insights/global%20energy%20perspective%202024/global-energy-perspective-2024.pdf (date of access: 10.08.2025).
8. Our Insights | Energy Solutions | McKinsey & Company [Electronic resource]. - Access mode: https://www.mckinsey.com/industries/oil-and-gas/how-we-help-clients/energy-solutions/our-insights (date of access: 10.08.2025).
9. 2025 Power and Utilities Industry Outlook | Deloitte Insights [Electronic resource]. - Access mode: https://www.deloitte.com/us/en/insights/industry/power-and-utilities/power-and-utilities-industry-outlook.html (date of access: 10.08.2025).
10. Hannan M. A. et al. Battery energy-storage system: A review of technologies, optimization objectives, constraints, approaches, and outstanding issues // Journal of Energy Storage. – 2021. – Vol. 42. https://doi.org/10.1016/j.est.2021.103023.
11. Mohammed A. Q., Al-Anbarri K. A., Jawad I. M. Metaheuristic Algorithm to Find Optimal Sizing of Stand-Alone Hybrid Energy System in Remote Areas: A Review //Wasit Journal of Engineering Sciences. – 2024. – Vol. 12 (4). – pp. 146-162.
12. Jain N. Application of deep reinforcement learning for real-time demand response in smart grids // International Research Journal of Modernization in Engineering Technology and Science. - 2025. - Vol. 7 (3). - pp. 2367 - 2375. https://doi. org/10.56726/IRJMETS6915.

13. Alomari, M.A.; Al-Andoli, M.N.; Ghaleb, M.; Thabit, R.; Alkawsi, G.; Alsayaydeh, J.A.J.; Gaid, A.S.A. Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions. Energies 2025. - Vol. 18. https://doi.org/10.3390/en18010141.
14. Nafees M. N. et al. Smart grid cyber-physical situational awareness of complex operational technology attacks: A review //ACM computing surveys. – 2023. – Vol. 55 (10). – pp. 1-36.
15. Ige A. B., Kupa E., Ilori O. Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources //International Journal of Science and Research Archive. – 2024. – Vol. 12 (1). – pp. 2978-2995.
16. Qiu X. et al. Levelized costs of the energy chains of new energy vehicles targeted at carbon neutrality in China // Frontiers of Engineering Management. – 2022. – Vol. 9 (3). – pp. 392-408.
17. Das V. et al. Optimal sizing and control of solar PV-PEMFC hybrid power systems //International Journal of Mathematical, Engineering and Management Sciences. – 2021. – Vol. 6 (4). – pp.1137-1156. https://doi.org/10.33889/IJMEMS.2021.6.4.068.
18. Optimum Design and Energy Management of Hybrid Power Generation Systems, Case Study: AL-Teeb District [Electronic resource]. - Access mode: https://systems.uomisan.edu.iq/library/uploads/files/3cpl9r5hxj6qm7b.pdf (date of access: 12.08.2025).
19. Bazmohammadi N. et al. Microgrid digital twins: Concepts, applications, and future trends //IEEE Access. – 2021. – Vol. 10. – pp. 2284-2302.
20. Jafari M. et al. A review on digital twin technology in smart grid, transportation system and smart city: Challenges and future //IEEe Access. – 2023. – Vol. 11. – pp. 17471-17484.
21. A Review of Digital Twin Technology and an Approach for a Robust Digital Twin for Power Systems Applications [Electronic resource]. - Access mode: https://curent.utk.edu/wp-content/uploads/2024/07/Till_Jeremy_UTK_Liu_1.pdf (date of access: 12.08.2025).
22. Thwe M. M. et al. Digital Twins for Power Systems: Review of Current Practices, Requirements, Enabling Technologies, Data Federation and Challenges //IEEE Access. – 2025. - Vol. 13. - pp. 105517 - 105540. https://doi.org/10.1109/ACCESS.2025.3580055.
23. Nambundo J. M. et al. Cybersecurity and Major Cyberthreats of Smart Meters: A Systematic Mapping Study. – 2025. - pp. 1-18. https://doi.org/10.20944/preprints202502.1399.v1.
24. Pinto, S.J.; Siano, P.; Parente, M. Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. Energies. - 2023. - Vol.16. https://doi.org/10.3390/en16041651.
25. Wasumwa S. A. Safeguarding the future: A comprehensive analysis of security measures for smart grids //World Journal of Advanced Research and Reviews. – 2023. – Vol. 19 (1). – pp. 847-871.
26. Talaat M. et al. Artificial intelligence applications for microgrids integration and management of hybrid renewable energy sources //Artificial Intelligence Review. – 2023. – Vol. 56 (9). – pp. 10557-10611.
27. Bareev-Rudy M., Schedler S., Clees T. Sizing optimization of hybrid hydrogen energy storage systems: A metamodel-based approach //International Journal of Hydrogen Energy. – 2025. https://doi.org/10.1016/j.ijhydene.2025.04.299.
28. Aguiar-Pérez J. M., Pérez-Juárez M. Á. An insight of deep learning based demand forecasting in smart grids // Sensors. – 2023. – Vol. 23 (3). https://doi.org/10.3390/s23031467.
29. Maurya P. K., Howard E. Artificial Intelligence to Enhance Energy Management and Distribution in Smart Grid Communication Networks //Tuijin Jishu/J. Propuls. Technol. – 2024. – Vol. 45. – pp. 4366-4378.
30. Eikeng E., Makhsoos A., Pollet B. G. Critical and strategic raw materials for electrolysers, fuel cells, metal hydrides and hydrogen separation technologies //International Journal of Hydrogen Energy. – 2024. – Vol. 71. – pp. 433-464.
31. Lencho N. G. et al. Techno-Economic Analysis of Green Hydrogen Production: A Review Focusing on the Geographical and Technological Factors //European Journal of Applied Science, Engineering and Technology. – 2025. – Vol. 3 (2). – pp. 233-260.
32. Benalcazar P., Komorowska A. Techno-economic analysis and uncertainty assessment of green hydrogen production in future exporting countries //Renewable and Sustainable Energy Reviews. – 2024. – Vol. 199. https://doi.org/10.1016/j.rser.2024.114512.
33. Zhang J., Bie Z., Zhang H. Faraday efficiency study of pressurized alkaline water electrolyzer // Electrochemical Society Meeting Abstracts 243. – The Electrochemical Society, Inc., 2023. – Vol. 36. – pp. 1966-1966.
34. Global Energy Perspective 2024 | McKinsey [Electronic resource]. - Access mode: https://www.mckinsey.com/industries/energy-and-materials/our-insights/global-energy-perspective (date of access: 15.07.2025).

35. EIA Annual Energy Outlook 2025 [Electronic resource]. - Access mode:https://www.jepic-usa.org/digests/2025/4/23/usa-eia-annual-energy-outlook-2025 (date of access: 15.07.2025).

36. Annual Energy Outlook 2025 [Electronic resource]. - Access mode: https://www.eia.gov/outlooks/aeo/ (date of access: 15.07.2025).

37. Song Z. et al. Digital twins for the future power system: An overview and a future perspective //Sustainability. – 2023. – Vol. 15 (6). https://doi.org/10.3390/su15065259.