(Online) ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 14, No. 1, March 2026, pp.213-226

Simulation-based approach to improving the functional stability of critical infrastructure objects under high-load stress conditions

Murat Kuanyshbayev[1], Yernar Akimbayev [2*], Zhakslyk Zhaguparov[3],
[1] Department of Civil Protection of the National Defense University of the Republic of Kazakhstan, Astana, Kazakhstan
[2] "Center for Applied Security Research" LLP, Astana, Kazakhstan
[3] Department of Emergency Protection at the Malik Gabdullin Academy of Civil Protection of the Ministry of Emergency Situations of the Republic of Kazakhstan, Kazakhstan

*Corresponding author E-mail: ernar_1974@mail.ru

ABSTRACT

Unified Power System (UPS) is an important critical infrastructure in Kazakhstan. Post-Soviet old designs, cyberattacks, natural disasters, and peak operational loads are the key risk factors. To ensure a good economic resilience and national security these structures have to be stable under extreme stress conditions. Therefore, the main objective of this paper is to use Monte Carlo simulations to evaluate the stability of Kazakhstan's smart grid infrastructure, under high-load scenarios. Seven scenarios were chosen in this work. These included a baseline case and two mitigation scenarios (capacity upgrade and demand management). In addition, four stress scenarios were analyzed including winter peaks, cyber-attack, renewable energy integration, and simultaneous transmission component outages. The system failure is defined as the occurrence of load demand exceeding allowable capacity limits. Results revealed the failure probability of the capacity upgrade scenario to be the lowest (1.5%) and the highest for cyber-attacks and simultaneous component outages scenarios (16.9%). The present research paper showed that probabilistic simulations can be used effectively to quantify the vulnerabilities in Kazakhstan's UPS.

Keywords: Monte Carlo simulation, smart grid resilience, critical infrastructure, high-load stress scenarios, Kazakhstan energy system.

1. Introduction

Critical infrastructures are large and complex systems made of many interconnected parts or smaller subsystems that work together. These infrastructures are called critical because their failure can lead to severe consequences. They provide essential services which society and economy rely on consistently. Transportation services, energy sector, water supply, public health, communication, and defense, are all considered as critical infrastructures. They face increasing threats in recent years such as, natural disasters, technical failures or cyberattacks. One can recall one of the examples of natural disasters "the 2021 Texas Power Crisis" where it exposed how vulnerable these infrastructures are to these sudden events [1]. Research has been mainly focusing on the causes and the way that these systems fail as well as their consequences. Many approaches and challenges have risen when addressing the protection of the critical structures. Marrone et al. [2] have made a system-level-approach where they proposed dealing with the structure entirely rather than isolated parts or subsystems. From a methodological point of view, Zio [3] pointed out on the dynamic nature of these systems and their variation over time, they also emphasized on the complexity of the components interaction.

In the Republic of Kazakhstan, the economy has maintained a remarkable steady, upward track since independence. Yet, it is still considered as a poor growth. The main cause is related to the old infrastructures of Soviet Union pipelines, which limits oil exportations [4]. In field of information technology, despite several

efforts in technological innovations (Like Enegix's 180 MW Data Center) [5], its digital and information infrastructures remain vulnerable. K. Azanbay [6] analyzed the main success and failure factors in the information security of Kazakhstan's republic. They showed that the key stresses include underdeveloped technical infrastructure, limited domestic electronics production, dependence on external technologies, and growing cybersecurity threats.

In the defense sector, Kazakhstan defense infrastructure show potential vulnerability when subjected to operational and technological stress. The main causes are the outdated production facilities and reliance on foreign technologies. Besides, the system was designed as a part of the Soviet union which lost critical supply chains after independence. Different studies have shown how logistical constraints weaken defense-related infrastructures when exposed to sustained disruption. Under complex or high pressure conditions project management, coordination and organizational structures failures reduce the adaptability of defense enterprises [7]. Defense sector also relies on other critical infrastructures like public infrastructures, as an example, Chung et al. [8] have proposed a methodology of quantifying the resilience of highways and railways in the US and shown how they affect directly the defense and military supply chains.

Smart grid system is also considered as a critical infrastructure which several sectors rely on its good operational capacity. In the republic of Kazakhstan, the integration of advanced digital technologies to manage electricity distribution have raised vulnerability to overloads and cyberattacks [9]. Due to a larger cyber-physical attack surface and increased reliance on automated control systems. Like the integration of renewable energy sources under the digital Kazakhstan program have amplified the risks of instability especially during peak demands [10]. It is well known that renewable energy sources are intermittent and present a limited dispatchability when demands exceeds available capacity. Several studies have shown that disruptions in smart grids can directly cascade to other areas such as defense and public services [11]. Thus, enhancing smart grid resilience is critical for ensuring other infrastructures stability.

To the best of our knowledge, simulation based national methodologies for assessing the stability and resilience of critical infrastructures in the Republic of Kazakhstan have not been identified in published or publicly available sources. Current research works do not integrate simulation techniques to limit and anticipate cascading failures or evaluate a system behavior under extreme conditions. Consequently, a significant research gap remains. Up to our knowledge, to date, no research has applied simulation approach to analyze Kazakhstani critical infrastructures under peak-load or high stress scenarios.

The impetus of this study is to develop a simulation-based approach exerting Monte Carlo simulation to evaluate the stability of Kazakhstan's smart grid energy infrastructure. Therefore, this study has used seven different scenarios, including baseline operations, capacity upgrades, and cyber-attack contingencies, the research focuses on key metrics such as stability indices and failure probabilities.

1.1. Literature review

Critical infrastructures' resilience received growing interest among researchers worldwide. The rise of cyberattacks, natural disasters, or intensive operational stresses has been the alarming call that pushed researchers to investigate resilience metrics and mitigation strategies [12]. Smart grids are among the most sensitive infrastructures to cascading failures. One disruption in a subsystem causes the entire network to fail. Their failure can simultaneously affect other sectors such as defense [13], healthcare [14], transportation, and economy [15]. Several studies have addressed the resilience through quantifiable metrics and scenario analysis. They showed that dynamic assessments, which account for time-dependent system behavior and operating conditions that evolve over time, provide insights beyond those offered by static reliability indices [16]–[18]. Ibne Hossain et al. [19] have developed a probabilistic graphical model (Bayesian network-based approach) to quantify the potential cyber risks on smart grid networks. They used various scenarios to identify the critical variables that enhances the cyber resilience of a smart grid system. Other approaches have been studied for the

cybersecurity of a smart grid systems including cryptography [20], graph theory [21], intrusion detection system [22], firewall system [23], etc…

Smart grid resilience with studies contrasting qualitative frameworks (conceptual frameworks,) and quantitative metrics (simulations) to evaluate system behavior under adverse conditions have been addressed. For example, Das et al. [24] provided a comprehensive review of resilience methods used to enhance real-world smart grids. They addressed the importance of using big data analysis frameworks of a smart grid simulator in order to better quantify its resilience.

Monte Carlo simulation is a simulation tool used for probabilistic assessment of a smart grid resilience. It's principle consists of using thousands of random scenarios to help identify the key vulnerable points. Smart grid resilience has been shown to be highly related to component failures, cyber intrusions, extreme weather, and load fluctuations [25]. In addition, several other studies have shown that Monte Carlo-based frameworks are suitable for evaluating smart grid performance under peak loads [25]–[27]. These simulations can also be applied for quantitative metrics. Narayan et al. have applied this method to derive resilience probability measures based on state transitions of Information and Communication Technology (ICT)-enabled grid services [28]. While Younesi et al. [29] have used it to evaluate resilience under extreme natural events in microgrid systems. The method is tested on standard power system models using many simulated disaster scenarios. This simulation method was successfully used to compute the resilience indicators and support decision-making for system planning and upgrades.

Multi-criteria decision-making methods, such as the Analytic Hierarchy Process (AHP), are frequently used to prioritize vulnerabilities and protection strategies [30]. However, AHP-based studies are often qualitative or semi-quantitative and are rarely combined with dynamic simulation.

To better capture cascading failures and interdependencies between power, communication, and control layers, several research works have used hybrid resilience models [31]–[33]. These models combine probabilistic simulation, graph theory, and cyber-physical modeling. However, despite their methodological sophistication these models remain largely theoretical.

Even though such amount of literature works has addressed quantitative and qualitative modeling on smart grids. In Kazakhstan, up to our knowledge, no peer-reviewed research has applied advanced simulation tools on smart grid infrastructure stability in the context of Kazakhstan's technological conditions. This lack of simple quantitative-based scenario tools hinders the ability of decision-makers to anticipate whether planned large-scale projects will perform successfully under stress conditions.

This justifies the urgent need for the present study, which seeks to develop an integrated simulation-based framework (using Monte Carlo method) to assess the vulnerability and stability of Kazakhstan's smart grid energy infrastructure under multi-factor stress scenarios.

2. Methodology

2.1. Object of study and data sources

This study has taken a national-level critical energy infrastructure in Kazakhstan, the "Unified Power System (UPS), operated by Kazakhstan Electricity Grid Operating Company (KEGOC), situated in Astana, Kazakhstan". The UPS has 144 power plants and 220-1150 kV transmission lines. The energy networks supply electricity to approximately 19 million habitants across 19 administrative regions.

The choice of this facility has been driven mainly because it has:

- The highest economic impact (71.6 TWh production, period from January to august 2025).
- Already shown overload vulnerabilities (as was the case for power outage in Almaty, June 19th [34]).
- Publicly available technical data.

The data used in this study are from publicly available sources, Table 1 shows each source and specifies which data it provides.

Table 1. Data sources and their role in the Monte Carlo simulation model.

Source	Data used	Role in simulation	Reference
stat.gov.kz https://stat.gov.kz/en/industries/business-statistics/stat-electric-power/stat-electric-power-2025/	Electricity production statistics (1150 MW Almaty average load 2025)	Input for Monte Carlo load generator	[35]
kegoc.kz https://ar2023.kegoc.kz/en/download/structure-of-the-company	UPS Development Plan 2023-2032 (1400 MW plant capacities, 2.8 GW RES)	Defines system capacity limits	[36]
SNiP RK 3.02-12-2003 https://prg.kz/document/?doc_id=31374795&pos=3;67	Electrical Installation Rules (110% overload limit)	Sets failure threshold	[37]
gov.kz / Ministry of Energy https://gov.kz/memleket/entities/energy?lang=en	Reliability indicators (SAIDI 118.4 min/yr)	Validation benchmark	[38]

2.2. Research design

In the present paper, a non-sequential Monte Carlo simulation was used to estimate the probabilistic reliability performance of the UPS under normal load distributions. The number of iterations were set to be 10^4 iteration. Various scenarios have been chosen (Baseline, Capacity upgrade, Demand management, winter peak, cyber-attack, Renewable Energy Sources (RES) integration, and the simultaneous loss of two critical system components "N-2 Contingency"), as shown in Table 2.

Table 2. Data sources and their role in the Monte Carlo simulation model.

Scenario	Parameters	Sources	Reference
S1: Baseline (1st scenario)	μ= 1150 MW, σ= 250 MW, C_{MAX}= 140 MW	stat.gov.kz Almaty 2025 loads	[35]
S2: Capacity upgrade (2nd scenario)	C_{MAX}= 1540 MW (+10%)	KEGOC Development Plan 2023-2032	[36]
S3: Demand management (3rd scenario)	μ= 1030 MW (− 10%)	Kazakh energy efficiency programs	[37]
S4: Winter peak (4th scenario)	σ= 375 MW (+50%)	Kazakh climate extremes (stat.gov.kz seasonal)	[38]
S5: Cyber-attack (5th scenario)	μ= 1300 MW (+ 13%)	KEGOC cybersecurity reports 2025	[36]
S6: RES integration (6th scenario)	σ= 350 MW	KEGOC 2.8GW renewable target	[36]
S7: N-2 Contingency (7th scenario)	μ= 1300 MW (double failure)	Engineering N-2 standard (KEGOC)	[36]

Load demand (denoted as: D_t) was modeled as a normal distribution $\mathcal{N}$ (μ=1150 MW, σ=250 MW) and is calculated using the following:

$$D_t \sim \mathcal{N}(\mu_t, \sigma_t) \quad (1)$$

Where: μ is the mean winter peak demand for Almaty UPS, and σ=250 MW.

The maximum generation capacity of the system is C_{MAX}. This parameter represents the upper limit of the system's capability to supply electricity. It is used to evaluate potential overloads. In the simulations, load demand is assumed to be constrained by C_{MAX} to ensure realistic operating conditions where: $D_t \leq C_{MAX}$.

The system failure is the overload event where the system demand exceeds the allowable operational capacity. The overload threshold is set to 110% of the nominal system capacity, based on national electrical regulations. The failure condition for each one is represented using an indicator function:

$$Failure_i \begin{cases} 1, L_i > 1.1 \times C_{MAX} \\ 0, otherwise \end{cases} \quad (2)$$

The performance indicator is the probability of failure. It quantifies the likelihood of system overload under each operating scenario. It is estimated as the sample mean of the indicator function. The probability of failure is calculated by:

$$P_f = \frac{1}{N} \sum_{i=1}^{N} Failure_i \quad (3)$$

Where N is the total number of iterations.

To ensure analytical rigor we have chosen seven scenario-specific assumptions. As shown in Table 2, the choice was based on publicly available data on Kazakhstan's energy infrastructure. Based on the reports of Almaty consumption patterns in 2025 (from stat.gov.kz), the baseline scenario was set. It assumes a normal load of μ=1150 MW and σ=250 MW. The capacity upgrade scenario was chosen as the second scenario, reflecting C_{MAX}=1540 MW (+10%), (KEGOC's Development Plan 2023-2032 for grid expansion). The third scenario chosen is demand management, it reduces mean load to μ=1030 MW (−10%). Winter peak scenario, which has been taken from the climate load profiles data [38]. The data include winter peak volatility to be increased to σ=375 MW (+50%), as summarized in Table 2. The cyber-attack scenario models a demand peak to μ=1300 MW (+13%), taken from the available data in "KEGOC cybersecurity reports 2025", control system disruptions [36]. It must be noted that, both S4 and S5 reflect the smart grid's infrastructure under high demand (high load) condition. Finally, the sixth and seventh scenarios representing RES integration and N-2 contingency scenarios, respectively, were taken from "KEGOC's engineering reliability standards for transmission security". We assume elevated volatility of σ=350 MW. And the N-2 contingency scenario sets μ=1300 MW for double-line failure.

2.3. Simulation model structure

In order to make sure of the results reproducibility of the current research, we adopted a simulation model structure represented through block diagrams, scenario tree, and mathematical formulas (Eq. 4-8). The following diagram (Figure 1) shows the blocks diagram of the simulation model structure. Input parameters, including load characteristics, system capacity (ie. Overload limit), and the number of Monte Carlo iterations, are first defined. A scenario is then selected from a predefined set of stress conditions (see Table 2). For each scenario, random load samples are generated and compared against the available system capacity. If the events exceeds thresholds, data is recorded and the performance indicators are calculated.

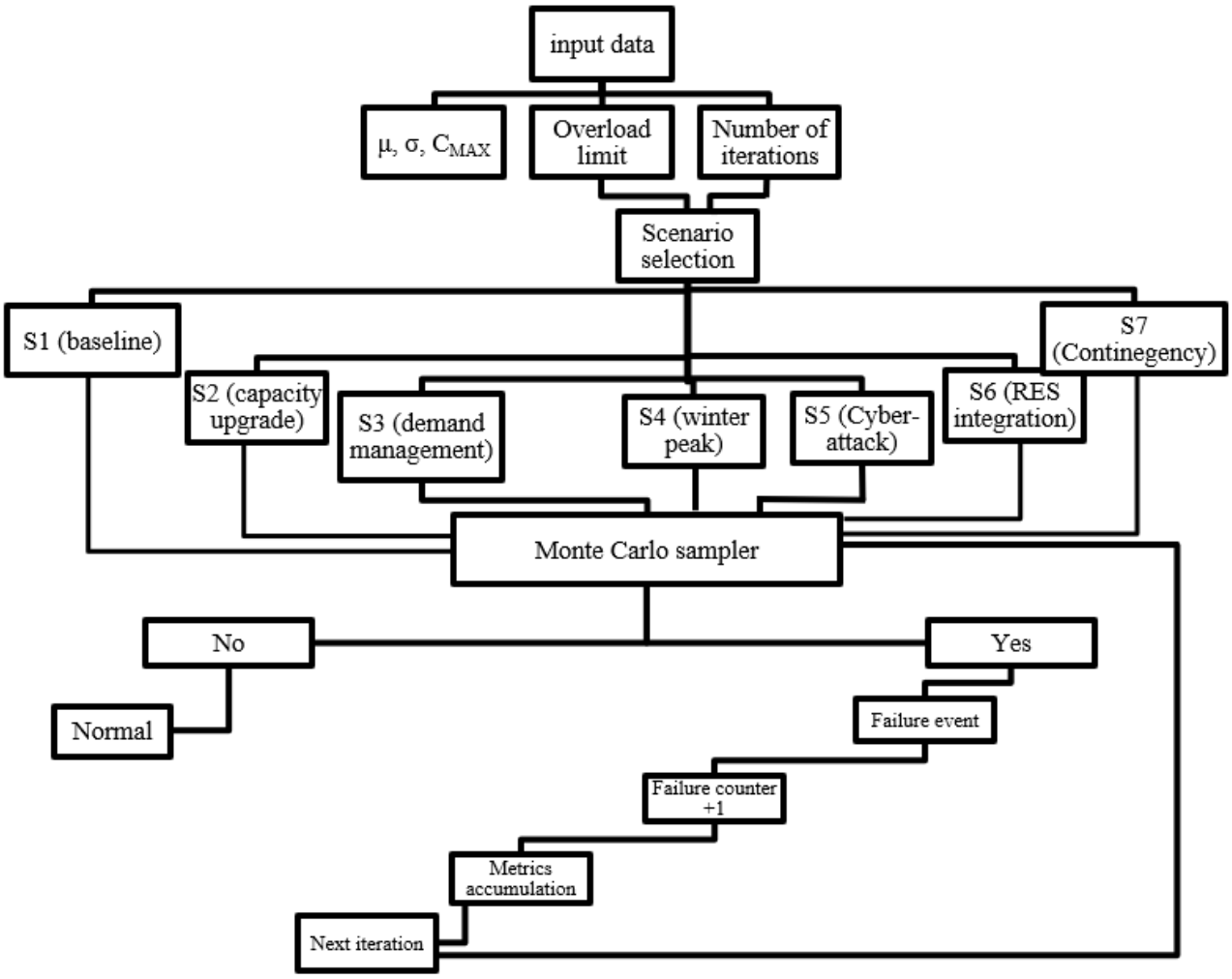

Figure 1. Monte Carlo simulation flowchart

Figure 2 shows the scenario tree for the Monte Carlo applied method. It illustrates the Kazakhstan UPS's stress conditions (under the seven different scenarios). As specified in previously in Table 2, these scenarios reflects specific modification in relation to the baseline values. Scenarios are applied independently and do not evolve over time.

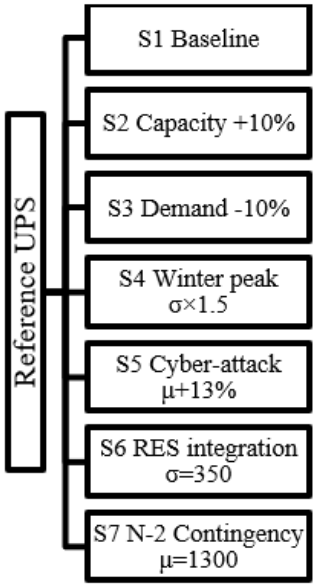

Figure 2. Scenario tree for the Monte Carlo simulation

2.3.1. Mathematical formulations

System demand is modeled as a stochastic variable. For each Monte Carlo iteration *i* under a predefined scenario *s*, the system load $L_i^{(s)}$ is sampled from a normal probability distribution:

$$L_i^{(s)} \sim N(\mu_s, \sigma_s) \tag{4}$$

Where μ and *s* are the scenario-specific mean load and standard deviation, respectively.

In accordance to the national electrical legislations, the threshold was set to 110% of the nominal capacity. This is the failure event, which its indicator is expressed as:

$$F_i^{(s)} = \begin{cases} 1, L_i^{(s)} > 1.1C_{MAX} \\ 0, \ otherwise \end{cases} \tag{5}$$

The number of iterations is N corresponding to 10^4 number of iterations. The primary performance indicator is the probability of failure, which quantifies the likelihood of system overload under each scenario. It is calculated as:

$$P_f^{(s)} = \frac{1}{N}\sum_{i=1}^{N} F_i^{(s)} \tag{6}$$

In addition, the Expected Load Not Supplied (ELNS) is computed to measure the average magnitude of overload:

$$ELNS^{(s)} = \frac{1}{N}\sum_{i=1}^{N} \max\left(L_i^{(s)} - C_{MAX}, 0\right) \tag{7}$$

A probabilistic downtime indicator is also estimated by scaling the probability of failure over a reference operating period:

$$D^{(s)} = P_f^{(s)} \times T_{ref} \tag{8}$$

Where T_{ref} represents the annual operating duration.

2.3.2. Model execution:

The simulation proceeds within each scenario by generating random load values. Failure conditions are systematically evaluated and the performance metrics are evaluated. Once the final number of iterations is attained, the indicators are aggregated to provide the system reliability under each stress condition.

Monte Carlo simulations were performed using Python 3.9. The non-sequential simulation framework executed 10,000 iterations per scenario, with normal distribution parameters and failure events as described in Table 2. Computational efficiency was achieved through vectorized operations, with each scenario completing in under 2 seconds on standard hardware.

2.4. Validation and sensitivity analysis

Validation is achieved with established engineering practices and national regulatory standards. The modeling criteria were chosen based on publicly available technical documents issued by Kazakhstan's grid operator (KEGOC) and national electrical installation standards (SNIP). SAIDI was used for reliability indicators recognition. This validation approach is commonly used in power system reliability studies.

For the sensitivity analysis, in short, the system is evaluated under modified load and capacity parameters. Calibration is done using publicly available empirical data extracted from documentation on Kazakhstan's energy system. Moreover, the overload conditions were derived from national electrical regulations. The aforementioned analysis ensures that the inputs reflect realistic operating conditions.

In this study no human participants nor personal data were used. Therefore, ethical approval is not applicable.

3. Results

Figure 3 shows the operational stability index obtained for the seven applied scenarios. The stability index values range from 57.4% to 95.9% for all scenarios. The highest stability index of 95.9 was recorded for the

demand management scenario (S3). It was followed by the capacity upgrade scenario (S2) having 94.8% stability index. The baseline scenario (S1) exhibits a stability index of 84.1%. Lower stability index values are observed for the winter peak scenario S4 (71.7%), the renewable energy integration scenario S6 (77.9%), and the N-2 contingency scenario S7 (61.3%). The cyber-attack scenario yields the minimum stability index value of 57.4%.

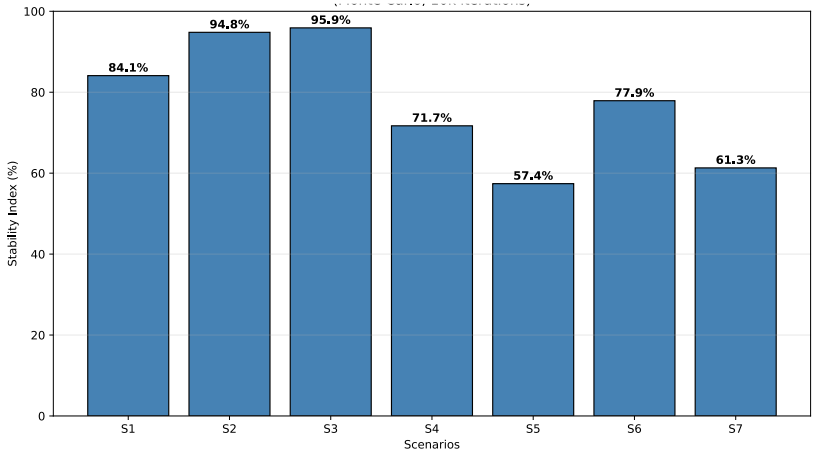

Figure 3. Operational stability index (100% − failure probability from Eq. 6), obtained from Monte Carlo simulation (10k iterations), under all scenarios. S1-Baseline, S2-Capacity upgrade, S3-Demand management, S4-Winter peak, S5-Cyber-attack, S6-Renewable energy integration, S7-N-2 contingency

The simulated load response distributions for all scenarios are shown in Figure 4. In each panel, the probability density of the system load is shown with the corresponding SNiP overload threshold (the red dashed line). For the first scenario "The baseline" the load distribution is concentrated between 800 MW and 1500 MW (x-axis) along with the SNiP threshold set at 1540 MW. It shows a symmetric distribution with a limited operlap beyond the threshold. It suggests a moderate risk under normal operating conditions. In the meanwhile, for the capacity upgrade scenario (S2), the SNiP threshold increases to 1694 MW, compared to S1. The third panel illustrating the S3 scenario showed a load distribution centered at lower demand levels compared to the baseline. Within this scenario it maintained the same SNiP threshold of 1540 MW.

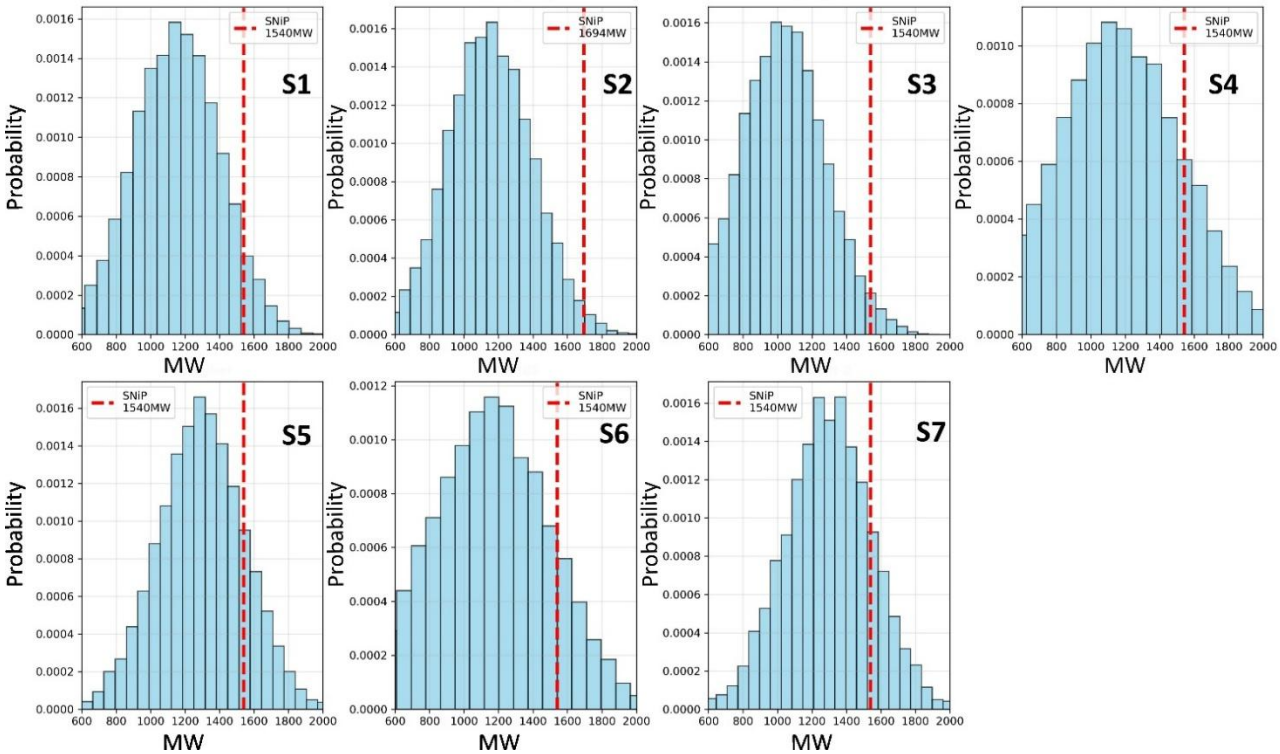

Figure 4. Load response curves by Scenario vs SNiP overload thresholds

The winter peak scenario (S4) and cyber-attacks (S5) showed a wider distribution with increased probability near the threshold. It showed high uncertainty-driven risk without a significant variation in the mean demand. Finally, the S6 and S7 scenarios are showing a distribution shifted toward higher loads with a concentration near the SNiP threshold of 1540 MW.

Figure 5 shows the cumulative distribution functions (CDFs) of simulated system load for all considered scenarios (obtained from Monte Carlo simulations). The vertical red dashed line in each panel refer to the SNiP overload threshold, which is defined as 1.1 C_{MAX}.

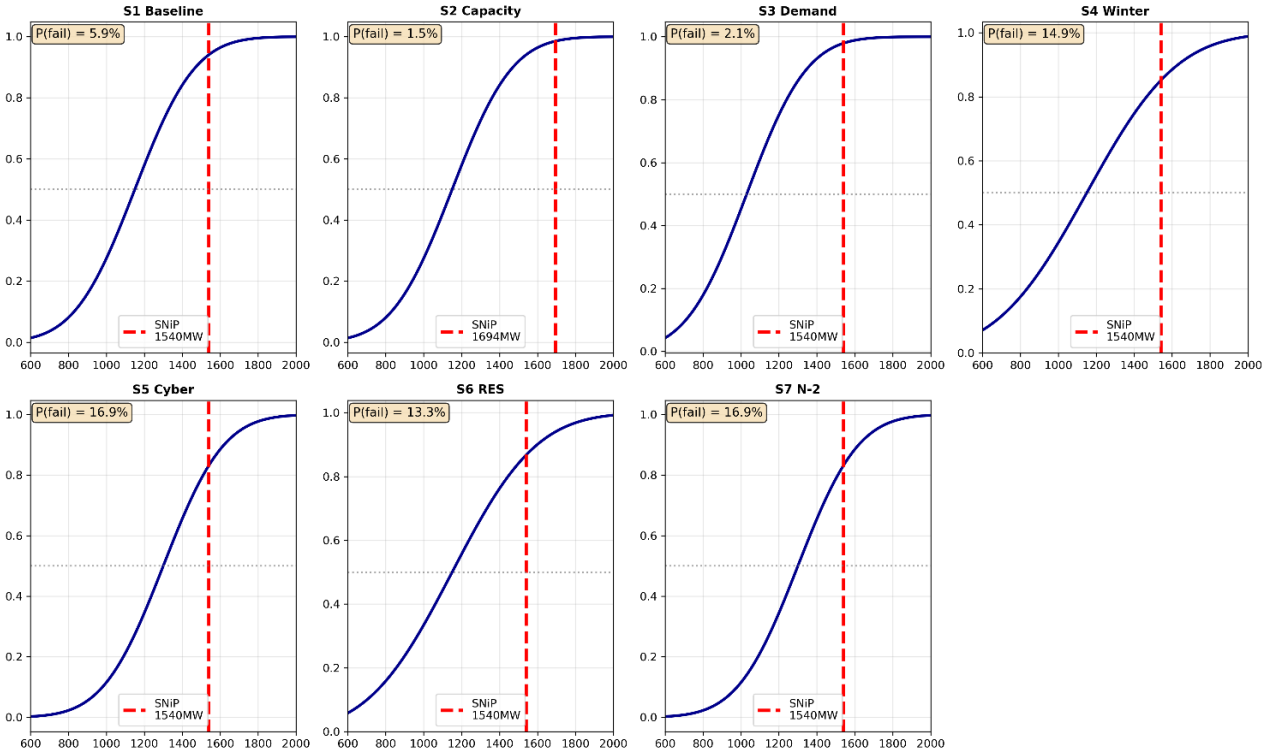

Figure 5. Cumulative distribution functions (P(D_t>1.1 C_{MAX}))

The resulting failure probabilities are summarized directly in the figure 5 and Table 3. The corresponding change in risk (ΔRisk) is recorded in percentages. The S1 scenario revealed a failure rate of 5.9%, which is used as the reference value for all upcoming comparisons. The Highest failure rates were obtained for the other scenarios: winter peak (14.9%), cyber-attack (16.9%), renewable energy integration (13.3%), and N-2 contingency (16.9%) scenarios. These high-risk scenarios resulted in positive ΔRisk values compared to the baseline (S1).

Table 3. Risk-level shift matrix (where the ΔRisk is the scenario risk- baseline risk, and pp=percentage points)

Scenario	Fail rate (%)	Baseline (%)	ΔRisk (pp)
Baseline (1st scenario)	5.9%	5.9%	+0.0pp
Capacity upgrade (2nd scenario)	1.5%	5.9%	−4.5pp
Demand management (3rd scenario)	2.1%	5.9%	−3.9pp
Winter peak (4th scenario)	14.9%	5.9%	+9.0pp
Cyber-attack (5th scenario)	16.9%	5.9%	+10.9pp
RES integration (6th scenario)	13.3%	5.9%	+7.3pp
N-2 Contingency (7th scenario)	16.9%	5.9%	+10.9pp

Figure 6 summarizes the load distribution statistics for all scenarios, including mean, standard deviation, and peak load values. Obviously, the median load is similar between the S1 and the S2 scenario, while the demand management (S3) showed the lowest median load. For the other scenarios, the load demands exhibited a large interquartile range.

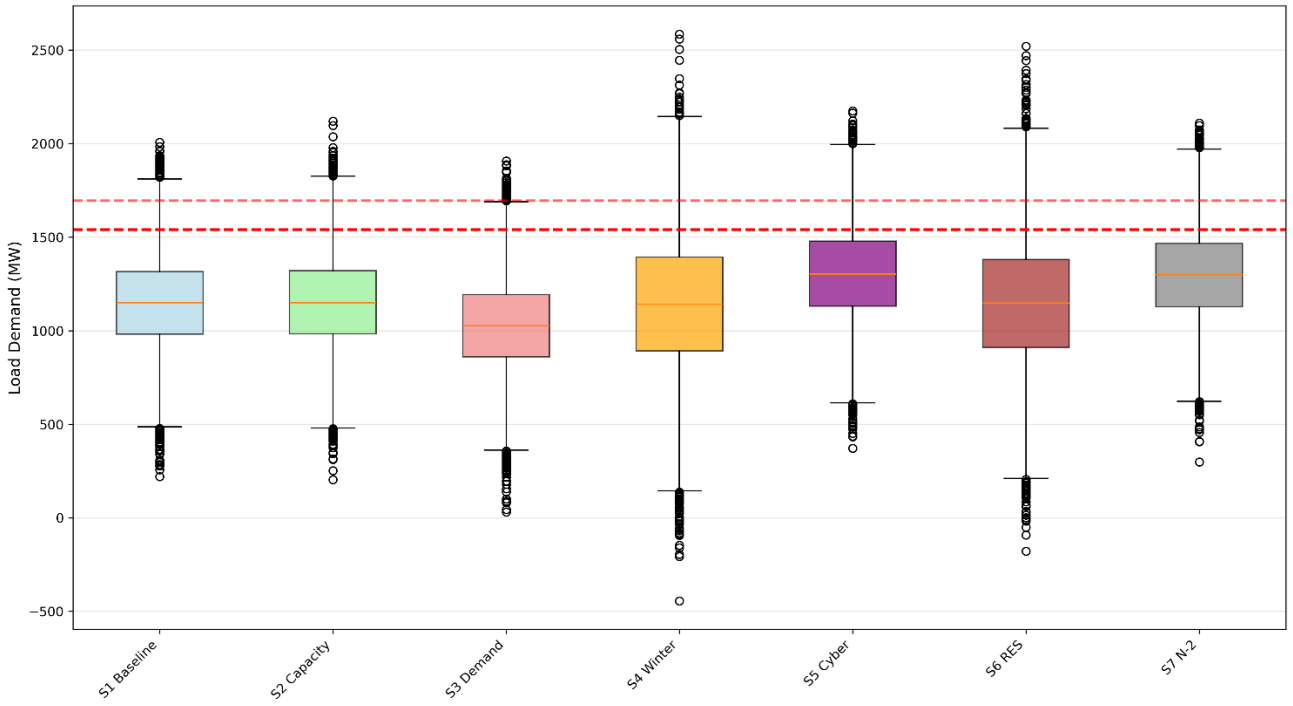

Figure 6. Load demand (MW) distribution vs. the corresponding scenario

4. Discussion

Based on the aforementioned results, the capacity upgrade scenario corresponded to 76% reduction while achieving 94.8% operational stability. These results show that SNiP standards are economically effective for normal and N-1 contingency conditions. Although comparable, the demand management achieved similar stability of 94.9% with a lower reduction in risk (3.9pp). The simulations on S3 showed a load-shedding effectiveness during peak conditions. On the other hand, cyber-attack (S5) and N-2 contingency (S7) scenarios increase failure risk by 10.9pp, reaching 16.9%, with stability indices dropping to critically low values of 57.4% and 61.3%, respectively.

Because of high-load demands, the winter peak conditions (S4) revealed an increased risk of +9.0pp. This has several causes; cold weather increases mechanical failures and gas pressure drops or frozen coal handling. This will result in a fuel supply interruptions meaning reduced generator availability which explains this scenario's failure.

Renewable energy integration (S6) produces moderate risk (+7.3pp), reflecting increased load variability under intermittent generation. In a power system, the net load becomes more variable when a large share of power plants production is intermittent. The remaining load that conventional generators must supply becomes more volatile, less predictable, and subject to sharper ramps. Thus, the system will show more variability even if the demand is unchanged. Overall, our results indicate that cybersecurity, contingency exposure, and extreme demand events are the primary vulnerabilities for Almaty UPS operations.

From a previous report on Eastern European urban UPS reliability, they reported a baseline typically ranges from 4–6% [39]. In the current paper, the baseline represents a 5.9% failure probability which fits within this range.

Concerning the cyber-attack scenario, it showed the highest failure probability of 16.9%. In the simulation, it means the loss of coordinated control and delayed response observed during cyber-induced disruptions of supervisory systems. In the case of the winter peak scenario, it showed a high risk values (+9.0 pp). This could be explained by the high demand levels during extreme cold periods. In Kazakhstan, some areas can reach −30 °C conditions, where it directly affects the power system overall performance. The moderate risk increase

observed under renewable energy integration (S6, +7.3 pp) arises from the variability rise in net system load. These results are in agreement with prior studies on high-renewable penetration networks [40].

By synthesizing all the previous results, the Almaty Unified Power System is highly affected by elevated stress conditions and low operational efficiency. The highest risks are noted for the cyber-induced disturbances and multiple contingency events. In its current state, the network struggles to respond effectively to sudden changes to high load stresses. Furthermore, seasonal demand fluctuations worsen this situation. Our findings suggest that the dominant sources of risk are not isolated technical faults, but rather a combined effect of demand variability, limited control flexibility, and network redundancy.

Limitations of the present research include the focus on a single UPS rather than the full Almaty network. In addition, the assumptions were made on a static load profile with fixed SNiP thresholds, and the absence of real-time control dynamics. Future works should extend Monte Carlo modeling to multi-UPS networks. Also, it needs incorporating dynamic reserve margins for real-time operational analysis.

5. Conclusions

The operational stability and risk behavior of the Almaty Unified Power System using Monte Carlo simulation method was evaluated. Seven different stress and mitigation scenarios were applied. The results show that capacity upgrades and demand management scenarios have a reduced failure probability, 1.5% and 2.1%, respectively. They both showed improved operational stability ~95% compared to the baseline. On the other hand, cyber-attack and N-2 contingency scenarios produce the highest failure probabilities and the lowest stability indices. Winter peak conditions and renewable energy integration scenarios also increase system risk, though to a lesser extent. Across all scenarios, quantitative metrics showed large variations in the system performance depending on stress type and mitigation strategy.

Herein, the results offer good predictive model for probability distribution and risk metrics for Kazakhstan's power system operators. Our findings suggest to prioritize the capacity reinforcement and grid hardening as an effective measure for reducing operational risks. Our results also emphasize on the need of cybersecurity and contingency management as the most vulnerable critical areas.

Future research should be oriented towards a multi-UPS and interconnected networks. Where incorporating dynamic reserve margins and real-time operational data is a must. Future work could also examine higher renewable penetration levels and create better protection strategies to improve smart grid's resilience.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

This article was prepared within the framework of a research project funded by the Ministry of Science and Higher Education of the Republic of Kazakhstan for the period 2024–2026 (IRN AP23489347, "Development of a model for improving the resilience of facilities to the damaging factors of modern means of destruction")

Acknowledgements

The author declares that there are no acknowledgements for this manuscript.

Author contribution

The contribution to the paper is as follows: Yernar Akimbayev: study conception and design; data collection; analysis and interpretation of results; draft preparation. The author approved the final version of the manuscript.

References

[1] N. M. Flores, H. McBrien, V. Do, M. V Kiang, J. Schlegelmilch, and J. A. Casey, "The 2021 Texas Power Crisis: distribution, duration, and disparities," *J. Expo. Sci. Environ. Epidemiol.*, vol. 33, no. 1, pp. 21–31,

2023, doi: https://doi.org/10.1038/s41370-022-00462-5.

[2] S. Marrone *et al.*, "Vulnerability modeling and analysis for critical infrastructure protection applications," *Int. J. Crit. Infrastruct. Prot.*, vol. 6, no. 3, pp. 217–227, 2013, doi: https://doi.org/10.1016/j.ijcip.2013.10.001.

[3] E. Zio, "Challenges in the vulnerability and risk analysis of critical infrastructures," *Reliab. Eng. Syst. Saf.*, vol. 152, pp. 137–150, 2016, doi: https://doi.org/10.1016/j.ress.2016.02.009.

[4] H. Yeo and J. S. Mah, "Industrial policy and diversification in the economic development of Kazakhstan," *Asian J. Soc. Sci. Manag. Stud.*, vol. 11, no. 2 SE-Articles, pp. 32–40, Jun. 2024, doi: https://doi.org/10.20448/ajssms.v11i2.5704.

[5] A. Kaskyrbekova, M. Yerken, A. Kaskyrbek, S. Lee, and I. Fakhradiyev, "The impact of Bitcoin mining on the carbon footprint in the Republic of Kazakhstan," *J. infrastructure, policy Dev.*, vol. 8, no. 11, pp. 1–11, 2024, doi: https://doi.org/10.24294/jipd.v8i11.7139.

[6] K. Azanbay, "Innovative Technologies as a Factor of Information Security of the Republic of Kazakhstan," *Ingénierie des Systèmes d'Information*, vol. 29, no. 2, pp. 523–532, 2024, doi: https://doi.org/10.18280/isi.290213.

[7] Y. N. Zabortseva, "From the 'forgotten region' to the 'great game' region: On the development of geopolitics in Central Asia," *J. Eurasian Stud.*, vol. 3, no. 2, pp. 168–176, 2012, doi: https://doi.org/10.1016/j.euras.2012.03.007.

[8] S. Chung, D. Sardak, M. Kitsak, A. Jin, and I. Linkov, "Contested logistics: Resilience of strategic highways and railways," *Transp. Res. Interdiscip. Perspect.*, vol. 32, p. 101507, 2025, doi: https://doi.org/10.1016/j.trip.2025.101507.

[9] T. K. Zhukabayeva, A. D. Adamova, N. E. Karabayev, V. A. Desnitsky, and N. S. Glazyrina, "Development of a penetration testing methodology for wireless networks to enhance smart city security in Kazakhstan," *Bull. L.N. Gumilyov Eurasian Natl. Univ. Math. Comput. Sci. Mech. Ser.*, vol. 149, no. 4 SE-, pp. 6–21, Dec. 2024, doi: http://doi.org/10.32523/bulmathenu.2024/4.1.

[10] N. T. Dolchinkov, "Interconnection of Digital, Cultural, and Strategic Transformations on the Balkan Peninsula." Achieving Business Excellence Through Triple Transformation, edited by Meltem Okur Dinçsoy and Hamit Can, IGI Global Scientific Publishing," 2025, pp. 209-240. doi: https://doi.org/10.4018/979-8-3693-9435-9.ch008.

[11] M. Z. Islam, Y. Lin, V. M. Vokkarane, and V. Venkataramanan, "Cyber-physical cascading failure and resilience of power grid: A comprehensive review," *Front. Energy Res.*, vol. Volume 11-2023, 2023, [Online]. Available: https://www.frontiersin.org/journals/energy-research/articles/10.3389/fenrg.2023.1095303

[12] A. Aghazadeh Ardebili *et al.*, "Enhancing resilience in complex energy systems through real-time anomaly detection: a systematic literature review," *Energy Informatics*, vol. 7, no. 1, p. 96, 2024, doi: https://doi.org/10.1186/s42162-024-00401-8.

[13] L. Chen, D. Yue, C. Dou, Z. Cheng, and J. Chen, "Robustness of cyber-physical power systems in cascading failure: Survival of interdependent clusters," *Int. J. Electr. Power Energy Syst.*, vol. 114, p. 105374, 2020, doi: https://doi.org/10.1016/j.ijepes.2019.06.032.

[14] J. A. Casey, M. Fukurai, D. Hernández, S. Balsari, and M. V Kiang, "Power Outages and Community Health: a Narrative Review," *Curr. Environ. Heal. Reports*, vol. 7, no. 4, pp. 371–383, 2020, doi: https://doi.org/10.1007/s40572-020-00295-0.

[15] I. Asensio Bermejo, H. Foretić, V. Kopustinskas, and G. Fulli, "Resilience assessment of a power system due to disruption of interconnectors," *Environ. Syst. Decis.*, vol. 45, no. 3, p. 48, 2025, doi: https://doi.org/10.1007/s10669-025-10041-2.

[16] M. Liu *et al.*, "Enhancing Cyber-Resiliency of DER-Based Smart Grid: A Survey," *IEEE Trans. Smart Grid*, vol. 15, no. 5, pp. 4998–5030, 2024, doi: https://doi.org/10.1109/TSG.2024.3373008.

[17] S. R. Salkuti, "Emerging and Advanced Green Energy Technologies for Sustainable and Resilient Future

Grid," *Energies*, vol. 15, no. 18. p. 6667, 2022. doi: https://doi.org/10.3390/en15186667.

[18] M. Ghanbari-Ghalehjoughi, K. Taghizad-Tavana, and S. Nojavan, "Resilient operation of the renewable energy and battery energy storages based smart distribution grid considering physical-cyber-attacks," *J. Energy Storage*, vol. 62, p. 106950, 2023, doi: https://doi.org/10.1016/j.est.2023.106950.

[19] N. U. Ibne Hossain, M. Nagahi, R. Jaradat, C. Shah, R. Buchanan, and M. Hamilton, "Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: a system of systems problem," *J. Comput. Des. Eng.*, vol. 7, no. 3, pp. 352–366, Jun. 2020, doi: https://doi.org/10.1093/jcde/qwaa029.

[20] P. Wang, Z. Lu, and Z. Tang, "An application of the Kriging method in global sensitivity analysis with parameter uncertainty," *Appl. Math. Model.*, vol. 37, no. 9, pp. 6543–6555, 2013, doi: https://doi.org/10.1016/j.apm.2013.01.019.

[21] A. A. Saad, S. Faddel, and O. Mohammed, "A secured distributed control system for future interconnected smart grids," *Appl. Energy*, vol. 243, pp. 57–70, 2019, doi: https://doi.org/10.1016/j.apenergy.2019.03.185.

[22] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Electr. Eng.*, vol. 67, pp. 469–482, 2018, doi: https://doi.org/10.1016/j.compeleceng.2018.01.015.

[23] P. Radoglou-Grammatikis, P. Sarigiannidis, T. Liatifis, T. Apostolakos, and S. Oikonomou, "An Overview of the Firewall Systems in the Smart Grid Paradigm," in *2018 Global Information Infrastructure and Networking Symposium (GIIS)*, 2018, pp. 1–4. doi: https://doi.org/10.1109/GIIS.2018.8635747.

[24] L. Das, S. Munikoti, B. Natarajan, and B. Srinivasan, "Measuring smart grid resilience: Methods, challenges and opportunities," *Renew. Sustain. Energy Rev.*, vol. 130, p. 109918, 2020, doi: https://doi.org/10.1016/j.rser.2020.109918.

[25] I. O. Guimarães, A. M. Leite da Silva, L. C. Nascimento, and M. Fotuhi-Firuzabad, "Reliability assessment of distribution grids with DG via quasi-sequential Monte Carlo simulation," *Electr. Power Syst. Res.*, vol. 229, p. 110122, 2024, doi: https://doi.org/10.1016/j.epsr.2024.110122.

[26] J. Xi, B. Zhang, and Y. Yang, "Calculation and Monte Carlo uncertainty analysis of the levelized cost of electricity for different energy power generation in the smart grid under time scales," *Energy Strateg. Rev.*, vol. 58, p. 101666, 2025, doi: https://doi.org/10.1016/j.esr.2025.101666.

[27] J. Faraji, M. Aslani, H. Hashemi-Dezaki, A. Ketabi, Z. De Grève, and F. Vallée, "Reliability Analysis of Cyber–Physical Energy Hubs: A Monte Carlo Approach," *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 848–862, 2024, doi: https://doi.org/10.1109/TSG.2023.3270821.

[28] A. Narayan, M. Brand, and S. Lehnhoff, "Quantifying the resilience of ICT-enabled grid services in cyber-physical energy system," *Energy Informatics*, vol. 6, no. 1, p. 23, 2023, doi: https://doi.org/10.1186/s42162-023-00287-y.

[29] A. Younesi, H. Shayeghi, A. Safari, and P. Siano, "Assessing the resilience of multi microgrid based widespread power systems against natural disasters using Monte Carlo Simulation," *Energy*, vol. 207, p. 118220, 2020, doi: https://doi.org/10.1016/j.energy.2020.118220.

[30] A. Almaleh, D. Tipper, S. F. Al-Gahtani, and R. El-Sehiemy, "A Novel Model for Enhancing the Resilience of Smart MicroGrids' Critical Infrastructures with Multi-Criteria Decision Techniques," *Applied Sciences*, vol. 12, no. 19. p. 9756, 2022. doi: https://doi.org/10.3390/app12199756.

[31] A. D. Syrmakesis, C. Alcaraz, and N. D. Hatziargyriou, "Classifying resilience approaches for protecting smart grids against cyber threats," *Int. J. Inf. Secur.*, vol. 21, no. 5, pp. 1189–1210, 2022, doi: https://doi.org/10.1007/s10207-022-00594-7.

[32] P. Asaridis, D. Molinari, F. Di Maio, F. Ballio, and E. Zio, "A probabilistic modeling and simulation framework for power grid flood risk assessment," *Int. J. Disaster Risk Reduct.*, vol. 120, p. 105353, 2025, doi: https://doi.org/10.1016/j.ijdrr.2025.105353.

[33] A. S. Mohamed, D. Kundur, and M. Khalaf, "A Probabilistic Approach to Adaptive Protection in the Smart

Grid," *ACM Trans. Cyber-Phys. Syst.*, vol. 9, no. 1, Jan. 2025, doi: 10.1145/3656347.

[34] R. Loginov, "Temporary Blackout Schedule Introduced in Central Almaty," *Orda English, 19-Jun-2025. [Online]. Available https//en.orda.kz/temporary-blackout-schedule-introduced-in-central-almaty-6975/. [Accessed December-2025].*, 2025.

[35] "Bureau of National Statistics of the Republic of Kazakhstan, Electricity production statistics," 2025. https://stat.gov.kz.

[36] "EGOC JSC, Unified Power System Development Plan for 2023–2032, Astana, Kazakhstan," 2023. https://www.kegoc.kz

[37] "Committee for Construction and Housing and Communal Services, SNiP RK 3.02-12-2003: Electrical Installation Rules, Republic of Kazakhstan," 2003.

[38] "Ministry of Energy of the Republic of Kazakhstan, Electric power system reliability indicators," 2024, [Online]. Available: https://www.gov.kz

[39] B. Roy and N. A. Ronald, *Reliability Assessment of Large Electric Power Systems*, 1st ed. Springer New York, NY, 1988. doi: https://doi.org/10.1007/978-1-4613-1689-3.

[40] X. Diao *et al.*, "Dynamic probabilistic risk assessment for electric grid cybersecurity," *Reliab. Eng. Syst. Saf.*, vol. 241, p. 109699, 2024, doi: https://doi.org/10.1016/j.ress.2023.109699.