Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume I, 273-277

An Integrated Approach to the Security of Energy Infrastructure: Problems and Innovative Solutions

Kiril Luchkov
Department of Economics, Industrial Engineering and Management
Technical University of Sofia
Sofia, Bulgaria
kiril.luchkov@tu-sofia.bg

Mihail Chipriyanov
Department of Strategic Planning
Tsenov Academy of Economics
Svishtov, Bulgaria
m.chipriyanov@uni-svishtov.bg

Galina Chipriyanova
Department of Accounting
Tsenov Academy of Economics
Svishtov, Bulgaria
g.chipriyanova@uni-svishtov.bg

***Abstract* — The study analyzes the security of energy infrastructure. The need for an integrated approach that overcomes the limitations of traditional security models is argued. Methodologically, a combination of system analysis, qualitative risk assessment and scenario modeling is applied. Through this approach, structural vulnerabilities are identified and threats are classified. The study establishes that the effectiveness of modern technological solutions depends on their integration with organizational and management mechanisms. An integrated security management model is proposed, aimed at increasing the resilience of energy infrastructure.**

Keywords* — *Artificial intelligence, Cyber-physical systems, Energy infrastructure, Resilience

I. Introduction

The security of energy infrastructure is being established as one of the central dimensions of modern national and international security [1]. Today, the energy sector is no longer an isolated industrial sphere and is becoming a complex, multi-layered socio-technical system [2]. Recent reviews further indicate that artificial intelligence is increasingly embedded in digital energy infrastructures through applications such as anomaly detection, predictive maintenance, forecasting and autonomous optimization [3]. Security is now a dynamic process requiring continuous adaptation.

Existing approaches and structures operate independently, without sufficient coordination in real time. Comparable studies in power-distribution mobile teams also demonstrate that algorithm-supported coordination can significantly improve response speed, resource deployment and operational effectiveness in critical network environments [4]. As a result, gaps in situational awareness are created that can be exploited in complex attacks. This problem reflects a structural deficiency in current security architectures. Hence the need for an integrated approach.

The present study aims to analyze the main problems related to the security of energy infrastructure and to propose a model for overcoming them. The main thesis is that the protection of energy systems in the context of hybrid threats can be achieved by encompassing the dimensions of security in a single analytical framework.

II. Theoretical and Literature Review

The concept of „energy security“ has traditionally been viewed as a function of the availability and access to energy resources. This approach has gradually proven to be insufficient. Cherp and Jewell propose a significant change. They define energy security as a state of low vulnerability of important energy systems [5]. This perspective allows the inclusion of new risks related to infrastructure interdependence and technological transformation. However, the proposed framework does not provide sufficient tools for the analysis of specific vulnerabilities.

A similar expansion of the analytical horizon is also observed in the research of Sovacool. He introduces an interdisciplinary approach. His analysis emphasizes that energy systems should be viewed as complex socio-technical structures. Technological solutions are related to the institutional and social context [6]. As a result, a gap is formed in the literature, in which the social dimensions are well developed and technological risks are partially investigated.

Panteli and Mancarella develop a model that considers resilience as the ability of energy systems to prepare for and recover from extreme events [7]. A flexible understanding of security is introduced. In this regard,

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol1.170

Humayed et al. emphasize that modern infrastructures function as cyber-physical systems [8].

Buldyrev et al. demonstrate that interdependent infrastructure systems are vulnerable to cascading failures [9]. This is especially true for energy infrastructure, which is closely linked to communication and information systems. Aven criticizes traditional probabilistic models of energy infrastructure [10]. Instead, he proposes a holistic approach.

Based on the identified problems, it is assumed that the security of energy infrastructure should be considered as a result of the interaction between technological, organizational and human factors. It is this logic that allows for the formulation of more effective protection models in conditions of increasing complexity and uncertainty.

III. MATERIALS AND METHODS

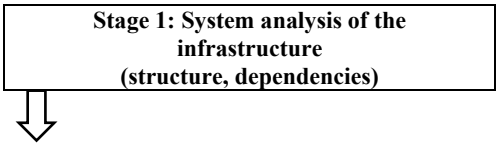
The present study is based on an integrated methodological approach. It combines systems analysis, qualitative risk assessment and scenario modeling. Related methodologies used in emergency-response teams further confirm the importance of coordinated decision systems under high uncertainty and time pressure [11]. The choice of this design is determined by the nature of the energy infrastructure, which functions as an interconnected socio-technical system. In such an environment, classical models prove to be insufficient. They do not take into account the interdependencies between physical and digital components. Therefore, a step-by-step analytical framework is applied. It allows a sequential transition from identifying vulnerabilities to formulating solutions. This approach ensures logical consistency and methodological clarity.

The proposed model is synthesized in Figure 1, which presents the logical structure of the study.

The figure illustrates the sequence of methodological stages, as well as the cyclical nature of the analysis, in which the results are used to update the initial model.

Stage 1: System Analysis of the Energy Infrastructure

The first stage of the methodology, presented in Figure 1, involves an analysis of the energy infrastructure. Here, it is viewed as a „system of systems“ including physical, digital and organizational components. The analysis covers the interaction between industrial control systems, supervisory control and data acquisition (SCADA) systems and physical energy assets. Particular attention is paid to important nodes and dependencies that can become points of failure. This approach identifies the structural vulnerabilities of the system. The result is an analytical map of the infrastructure, which serves as the basis for the following stages.



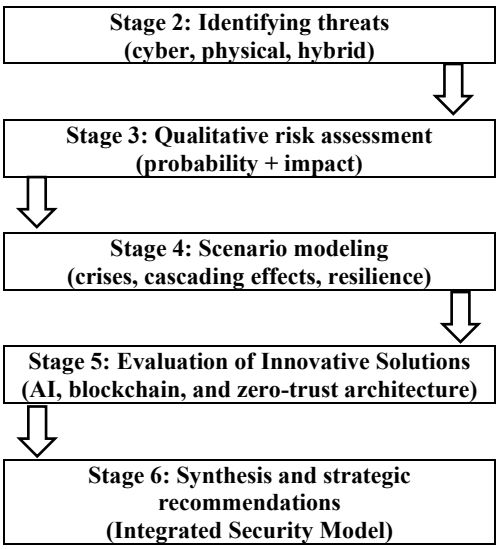


Fig. 1. Methodological model for analyzing the security of energy infrastructure

Source: Authors' own research.

Stage 2: Identification and Classification of Threats

The second stage builds on the system analysis by identifying threats. They are classified as cyber, physical and hybrid, in accordance with the logic presented in Figure 1. The analysis includes the development of typical impact scenarios. This allows for a transition from theoretical to applied analysis. As a result, a structured typology of threats is formed. This typology is decisive for the risk assessment.

Stage 3: Qualitative Risk Assessment

The third stage reformulates the identified threats into assessable risks. A qualitative approach is used, based on two criteria - probability and impact. Risks are classified into categories, which allows prioritization of protective measures. Particular attention is paid to events with low probability but high impact. This stage is a central part of the model. It connects the analysis with management decisions. The approach is consistent with the integrated logic of the methodology. The result is a clear picture of the risk profile.

Stage 4: Scenario Modeling and Resilience

The fourth stage involves the development of crisis scenarios and analysis of the system's resilience. The scenarios cover different types of attacks and failures, including hybrid impacts. The behavior of the system under different conditions is analyzed. Particular attention is paid to cascading effects. The results support the development of solutions.

Stage 5: Evaluation of Innovative Solutions

The fifth stage is aimed at evaluating modern technological solutions, such as artificial intelligence, blockchain and zero-trust architecture. Their ability to improve security is analyzed. Their applicability in a real environment is assessed. Of particular importance is their

integration with existing systems. This stage connects theory with practice. This stage represents the main contribution of the study.

Stage 6: Synthesis and Strategic Recommendations

The final stage summarizes the results and formulates strategic directions. The emphasis is on an integrated approach. The recommendations are aimed at increasing resilience. In this stage, the overall model is formed. It can be applied at different levels. This completes the methodological framework.

IV. RESULTS

The application of the methodological model (Figure 1) allows us to provide an analytical characterization of the structural properties of risk in the energy infrastructure. Already at the level of the system analysis, it is established that the vulnerability is not evenly distributed. The disruption of the functionality of digital management systems does not lead to local effects, but to the propagation of effects throughout the system. This means that the risk has a clearly expressed structural logic and cannot be considered as a random phenomenon. The analysis also shows that digitalization increases the density of these dependencies. Security management becomes increasingly complex. Thus, the first justified conclusion is formulated: the resilience of the system is a function of its internal structure, and not only of external protective mechanisms.

TABLE 1 RISK PRIORITIZATION BASED ON THE PROBABILITY-IMPACT RATIO

Threat	Rating
SCADA attack	Medium probability, high impact
Physical sabotage	Low probability, very high impact
Hybrid attack	Low probability, critical impact
Internal threat	Medium probability, medium impact
Legacy systems	High probability, medium impact

Source: Authors' own research.

The highest risk arises in scenarios where cyber attacks are transferred to the physical level. This is realized in the direction of industrial control systems and supervisory control and data acquisition (SCADA) systems. As a result, their vulnerability has a multiplier effect and increases the likelihood of failures. Additionally, it is established that hybrid threats do not necessarily require high technological complexity [12]. This highlights the need for more effective coordination of different types of impact. At the same time, it is observed that internal threats and legacy systems further enhance vulnerability by creating conditions for an initial breakthrough. The synthesized risk assessment is presented in Table 1.

The data summarized in Table 1 highlight a paradox in modern energy infrastructure security: the threats with the highest potential impact often have lower predictability. For example, "legacy systems" present a high probability of exploitation due to outdated software and unpatched vulnerabilities. Yet their impact remains categorized as medium, as their failure modes are typically localized. "Hybrid attacks" and "physical sabotage" exhibit low probability combined with very high impact, capable of causing system outages. A shift to predictive and intelligence-driven security operations is required. This will favor the allocation of mitigation resources in proportion to the systemic severity of the risk, not just its frequency.

Risk assessment and scenario modeling reveal that the behavior of the system is characterized by the presence of cascading effects [14]. This creates serious difficulties in the early detection of threats. The analysis shows that this phase is the most important for risk management. As a result, it is confirmed that classical security indicators are not sufficient to assess the real state of the system. The results of the individual stages are summarized in Table 2.

TABLE 2 COMPARISON OF METHODOLOGICAL STAGES WITH THE OBTAINED ANALYTICAL RESULTS

Stage	Conclusion
System analysis	High interdependence
Identifying threats	Dominance of hybrid risks
Risk assessment	Prioritize high-impact events
Scenarios	Nonlinear propagation of effects
Technologies	Limited stand-alone effectiveness
Synthesis	An integrated model is needed

Source: Authors' own research.

Table 2 demonstrates that each step of the methodology leads to a qualitatively new level of understanding of risk. This allows us to formulate a third conclusion: security should be viewed as a dynamic process. Such an approach requires continuous adaptation of protection strategies. In this context, resilience becomes a key criterion for system effectiveness.

Blockchain technologies provide a high level of data integrity. More broadly, studies on reporting systems also confirm that data integrity and transparent information flows are central elements of effective governance architectures [13]. However, they cannot help in cases of physical vulnerabilities. Zero-trust architecture limits the spread of attacks, but requires a significant transformation of organizational processes. The summarized assessment is presented in Table 3.

TABLE 3 FUNCTIONAL ROLE OF INNOVATIVE TECHNOLOGIES IN SECURITY MANAGEMENT

Technology	Functional Role	Detection Efficiency	Implementation Complexity	Cost	Risk Level	Maturity

AI	Anomaly detection	High	High	High	Medium	Medium
Blockchain	Data integrity	Medium	Medium	Medium	Low	High
Zero Trust Architecture	Restrict access	High	Very High	High	Medium	High
Algorithmic Coordination	Response support	High	Medium	Low	Low	High

Source: Authors' own research.

Multidimensional metrics (from Table 3) provide a comprehensive overview of operational and economic trade-offs. Innovative tools such as artificial intelligence and Zero Trust architecture offer high detection efficiency. At the same time, they require significant financial investments and present moderate organizational risks during implementation. Specialized solutions such as algorithmic coordination demonstrate a high level of technological maturity, which is combined with low risks during implementation. This makes them highly applicable to increasing network resilience. This assessment emphasizes that the selection of security technologies requires a balanced analysis of asset vulnerability, available budget and levels of systemic risk.

The effectiveness of technologies depends on their integration into the system. Their impact remains limited without coordination with organizational and management mechanisms. Solutions require integration. This sequence represents the main analytical contribution of the study. It allows the construction of a more precise security management model that takes into account the real complexity of the energy infrastructure. In this sense, the study offers a reasonable framework for its solution.

According to threat intelligence reports (such as IBM X-Force), the energy sector is among the top 3 most attacked industries. It accounts for 11% to 14% of all cyberattacks. Three macro trends support our model:

- OT Exploitation: Attacks against operational technologies (ICS/SCADA) are growing by over 25% annually, demonstrating the migration of threats to the physical layer.
- Ransomware and Extortion: Ransomware accounts for nearly 30% of incidents in the sector, escalating into hybrid extortion and physical sabotage threats.
- Geopolitical APT Aspects: Over 65% of sophisticated attacks are state-sponsored, relying on supply chain compromise and algorithmic manipulation.

With the expected 35% growth in smart grid devices over the next 5 years, traditional defenses are becoming obsolete. Modern risks require an architecture that combines zero-trust management, technical protection, and algorithmic team coordination.

V. DISCUSSION

The results obtained require a reassessment of the leading theoretical and practical approaches to the security of energy infrastructure. In the framework of this study, it was found that vulnerability is structurally concentrated. The results confirm the need to move to an integrated security model, in which the interactions between components are at the center of the analysis. Such an interpretation corresponds to the line in the studies of Cherp and Jewell. They emphasize vulnerability as the main criterion for energy security. The present study builds on this perspective because it concretizes it in cyber-physical systems. Thus, a higher degree of operationalization of the concept of „vulnerability" is achieved.

The results show that the combined scenarios generate the highest level of risk. This observation questions the adequacy of existing classification models that distinguish threats by type without taking into account their mutual change. In this context, the vulnerabilities of industrial control systems (including SCADA systems) acquire leading importance. This confirms the thesis that the security of energy infrastructure should be considered as a cyber-physical phenomenon.

The present study supports the transition to a model based on resilience and continuous risk management. This means that security should be considered as a process.

VI. CONCLUSIONS

Based on the study, several specific scientific conclusions can be formulated that contribute to the development of the existing theoretical framework. First, the vulnerability of the energy infrastructure is structurally determined and concentrated in a limited number of points. Second, the leading risk arises from hybrid threats. Third, the behavior of the system in crises requires the use of scenario models for analysis. Fourth, the effectiveness of technologies depends on their integration into organizational and management processes. Fifth, resilience should be considered as a fundamental security criterion. Sixth, the lack of coordination between different levels of management is a significant factor for vulnerability.

One particularly defining area for future research is the specific analysis of high-risk AI systems in cyberattacks. This is the case when they are directed against critical energy infrastructures. Today, artificial intelligence (AI) is increasingly integrated into operational technologies. As a result, assessing the vulnerabilities of these high-risk algorithms against sophisticated cyberthreats will be

essential for maintaining system stability and preventing cascading network failures in the future.

At the strategic level, a move should be made to building comprehensive security management models [15]. This implies the development of policies that encourage coordination between different institutions and infrastructure operators. At the organizational level, mechanisms for real-time information exchange should be created.

VII. ACKNOWLEDGMENTS

This research was funded by the Bulgarian National Science Fund at the Ministry of Education and Science of Bulgaria under the Funding Competition for Fundamental Scientific Research Projects 2025, based on Administrative Contract № KP-06-N95/16 of 10 December 2025, for the implementation of Research Project № KP-06-PN95/45, SUNI № BG-175467353-2025-08-0248, titled „Epistemic robustness of artificial intelligence: A universal framework for evaluation in industrial and management systems“.

REFERENCES

[1] Li, Q., & Song, Z., Research on Energy Security in the EU from a Trade Perspective: A Historical Analysis from 1991 to 2021. Energies, 18(14), 2025, 3801. https://doi.org/10.3390/en18143801

[2] Papamichael, I., Voukkali, I., Vrionides, K., Loizia, P., Stylianou, M., Sospiro, P., Liscio, M. C., Naddeo, V., & Zorpas, A. A., An overview of critical energy infrastructure of the European Defence sector, Energy Nexus, Volume 19, 2025, 100483, ISSN 2772-4271, https://doi.org/10.1016/j.nexus.2025.100483.

[3] Zinoviev, V., Koeva, D.; Tsankov, P., Kutkarska, R. Review of Artificial Intelligence Applications in the Digital Energy and Renewable Energy Infrastructures. Energies 2026, 19, 1250. https://doi.org/10.3390/en19051250

[4] Angelova, M., Anguelov, K., Indicators for Evaluating the Effectiveness of Algorithmic Management in Mobile Teams of Power Distribution Companies, 19th Conference on Electrical Machines, Drives and Power Systems (ELMA), Sofia, Bulgaria, 2025, pp. 1-4, doi: 10.1109/ELMA65795.2025.11083518.

[5] Cherp, A., & Jewell, J., The concept of energy security: Beyond the four As, Energy Policy, Volume 75, 2014, Pages 415-421, ISSN 0301-4215, https://doi.org/10.1016/j.enpol.2014.09.005.

[6] Sovacool, B. K., Evaluating energy security in the Asia Pacific: Towards a more comprehensive approach. Energy Policy, 39(11), 2011, Pages 7472-7479. https://doi.org/10.1016/j.enpol.2011.09.008.

[7] Panteli, M., & Mancarella, P., The grid: Stronger, bigger, smarter? Presenting a conceptual framework of power system resilience. IEEE Power and Energy Magazine, 13(3), 2015, Pages 58-66. https://doi.org/10.1109/MPE.2015.2397334

[8] Humayed, A., Lin, J., Li, F., & Luo, B., Cyber-physical systems security - A survey. IEEE Internet of Things Journal, 4(6), 2017, Pages 1802-1831. https://doi.org/10.1109/JIOT.2017.2703172

[9] Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S., Catastrophic cascade of failures in interdependent networks. Nature, 464, 2010, Pages 1025-1028. https://doi.org/10.1038/nature08932

[10] Aven, T., Risk assessment and risk management: Review of recent advances on their foundation, European Journal of Operational Research, Volume 253, Issue 1, 2016, Pages 1-13, ISSN 0377-2217, https://doi.org/10.1016/j.ejor.2015.12.023.

[11] Angelova, M., Anguelov, K., Methodology for Evaluation Effectiveness and Efficiency of Algorithmic Management in Emergency Response Teams, 19th Conference on Electrical Machines, Drives and Power Systems (ELMA), Sofia, Bulgaria, 2025, pp. 1-5, doi: 10.1109/ELMA65795.2025.11083484.

[12] Abraham, D., Houmb, S. H., & Erdodi, L., Cyber-Attacks on Energy Infrastructure - A Literature Overview and Perspectives on the Current Situation. Applied Sciences, 15(17), 9233, 2025. https://doi.org/10.3390/app15179233

[13] Stoyanov, P., Anguelov, K., Corporate Social Responsibility Reporting: Information System Requirements, 13th International Scientific Conference on Computer Science (COMSCI), Sozopol, Bulgaria, 2025, pp. 1-5, doi: 10.1109/COMSCI67172.2025.11225210.

[14] Wu, X., Zhao, S., Shen, Y., Madani, H., & Chen, Y., A Combined Multi-Level Perspective and Agent-Based Modeling in Low-Carbon Transition Analysis. Energies, 13(19), 2020, 5050. https://doi.org/10.3390/en13195050

[15] D. Petrova. Intelligent, Innovative and Sustainable Industry in Bulgaria – prospects and challenges, Vide I. Tehnologija. Resursi - Environment, Technology, Resources, Proceeding of the 12th International Scientific and Practical Conference „Environment. Technology. Resources“, June 20-22, 2019, Rezekne, Latvia, Volume I, pp. 210-215, ISSN 1691-5402 – print, ISSN 2256-070X – online. https://doi.org/10.17770/etr2019vol1.4188