Annual International Scientific Conference
"Competitiveness and Innovation in the Knowledge Economy"
September 26-27, 2025
Chisinau, Republic of Moldova

DOI: https://doi.org/10.24818/cike2025.67

STOCHASTIC MODELING OF CYBER THREAT RISKS IN SMART GRIDS AS A TOOL OF ECONOMIC CYBERNETICS

CONIUC SVETLANA
S.C. ADD-PRODUCTION S.R.L., Chisinau, Moldova
e-mail: svetlana.coniuc@gmail.com
ORCID ID: 0009-0003-6796-9940

RUSANOV ALEXEY
S.C. ADD-TECHNOLOGY S.R.L., Chisinau, Moldova
e-mail: rusanov.alexei@gmail.com
ORCID ID: 0000-0001-6573-9242

Email addresses of corresponding author: svetlana.coniuc@gmail.com

Abstract. The development of smart grids represents a fundamental direction in the digitalization of infrastructure within the knowledge economy. Smart grids enable efficient distribution of energy resources, integration of renewable sources, and real-time interaction between consumers and suppliers. However, the openness of their information and communication architecture significantly increases vulnerability to cyber threats. Attacks on power networks may cause not only technological disruptions but also large-scale economic losses, directly affecting the competitiveness of both states and enterprises.

This paper emphasizes Smart Grid security as a critical factor of economic resilience. Economic cybernetics provides a methodological basis for assessing risks, while stochastic modeling offers quantitative tools for evaluating cyber threat probabilities and optimizing defense strategies. Methods such as Markov chains, Poisson processes, and stochastic Petri nets are applied to describe system state transitions, attack intensities, and interdependencies of infrastructure components.

The main results of the study demonstrate that stochastic models allow the formalization of cyber threats in probabilistic terms, prediction of incident dynamics, calculation of resilience indicators, and justification of optimal investment levels in cyber defense. Furthermore, the integration of such results into economic management models enhances decision-making efficiency in balancing innovation, costs, and infrastructure stability.

In conclusion, stochastic risk modeling contributes not only to the reliability and resilience of Smart Grids but also to the broader field of economic cybernetics, where mathematical methods support effective governance of socio-economic systems under conditions of cyber vulnerability.

Keywords: Smart Grids, Cybersecurity, Stochastic Modeling, Economic Cybernetics, Risk Assessment, Resilience
JEL Classification: C02, C61, O33, Q43

1 Introduction

The digitalization of the energy sector today stands as one of the key directions in the development of the knowledge economy. It involves not only the introduction of intelligent technologies into the processes of electricity generation, transmission, and distribution, but also the creation of new models of interaction between producers and consumers. Within this paradigm, a special role is played by Smart Grids, which ensure efficient resource distribution, the integration of renewable energy sources, and two-way real-time communication (Y. Yan *et al., 2012*). Unlike traditional power systems, where energy transmission processes remain relatively isolated from information support, Smart Grids are established as cyber-physical infrastructures in which energy and information flows are inseparably connected and mutually influence one another. (X. Fang *et al.,* 2012)

This integration opens new opportunities for improving energy efficiency, resilience, and infrastructure reliability. Through the use of intelligent algorithms for forecasting and load distribution, it becomes possible to minimize losses, increase the share of "green" generation, and optimize the interaction of all market participants. At the same time, however, the level of vulnerability also increases: the openness of the information architecture and the high degree of interdependence create favorable conditions for cyberattacks (A. R. Metke *et al.,* 2010). Disruptions in the operation of Smart Grid digital components can lead not only to local failures but also to large-scale technological accidents capable of causing significant economic losses. Such incidents affect both the resilience of national energy systems and the competitiveness of individual enterprises and entire states. (H. He *et al.,* 2016)

Under these conditions, ensuring the cybersecurity of Smart Grids becomes a strategic priority. The successful development of Smart Grids is impossible without comprehensive approaches to risk management, in which economic cybernetics plays a key role. It provides the methodological foundation for analyzing threats, assessing the probabilities of incidents, and identifying the optimal balance between innovative development and infrastructure protection costs. In turn, stochastic modeling offers tools for quantitative analysis: it makes it possible to formalize the dynamics of cyberattacks in probabilistic terms, predict the escalation of incidents, and evaluate system resilience indicators. (Y. Mo *et al.,* 2012)

Thus, a comprehensive assessment of Smart Grid cyber resilience requires the combination of both technical and economic approaches. The methodology proposed in this article is based on stochastic modeling and is aimed at creating an integrated analytical framework that considers not only the technical aspects of power system functioning but also the economic feasibility of investments in protective measures. Such a synthesis makes it possible not only to identify and predict threats but also to substantiate strategies for the development of digital energy with due regard for cyber risks.

2 Literature Review and Problem Statement

Contemporary research convincingly demonstrates the growing threat of cyberattacks targeting critical energy infrastructure. Smart Grids, as a central element of the digital transformation of the energy sector, are becoming the object of increasingly sophisticated attacks aimed at compromising data integrity, disrupting control processes, and undermining trust in energy systems as a whole. A number of analytical surveys on Smart Grid cybersecurity highlight typical vulnerabilities. Among them are insufficiently protected communication channels (both wired and wireless), which are susceptible to data interception and substitution; asynchronous notification mechanisms, designed to transmit critical messages but potentially exploited for injecting false information; and the high likelihood of cascading failures triggered by the spread of distorted telemetry data. Such threats indicate that even a local malfunction may escalate into a systemic crisis.

At the same time, international standards and best practices in the field of critical infrastructure protection emphasize the necessity of resilience-oriented design (K. A. Shcheglov *et al.,* 2014). This approach is concerned not only with preventing attacks but also with ensuring that the energy system can maintain operability in their occurrence, rapidly detect incidents, and recover with minimal losses. A crucial element here is the balance between risk management and investment efficiency: resources must be allocated in such a way as to minimize the probability of catastrophic consequences while avoiding excessive expenditures with low returns.

Despite significant progress, most existing studies focus primarily on threat identification and vulnerability classification, while insufficient attention is paid to comprehensive analysis that includes mathematical modeling of attack dynamics, the assessment of operational reliability indicators, and the integration of these results with economic decision-making mechanisms. The

absence of a unified model leads to fragmented approaches and complicates the development of optimal protection strategies (K. A. Shcheglov *et al.,* 2012).

This article seeks to bridge this gap. The proposed approach combines probabilistic (stochastic) modeling, which enables the formalization of cyberattack processes and their impact on power system resilience, with economic analysis of investment efficiency in protective measures. Such an integrated methodological framework provides a foundation for developing solutions that simultaneously take into account the technical characteristics of power grids, economic constraints, and the requirements for ensuring resilience under increasing cyber threats.

3 Methodology

To formalize the processes occurring in Smart Grids under cyberattacks, this study employs stochastic modeling based on Continuous-Time Markov Chains (CTMC). This approach makes it possible to describe the probabilistic transitions of the system between different operational states, taking into account both external impact factors and internal recovery processes (K. A. Shcheglov *et al.,* 2014).

The model distinguishes four basic states:

S_0 – Normal operation: all data remain reliable, control is carried out correctly, and the system functions in normal mode.

S_1 – Local compromise: a subset of devices (e.g., individual meters or concentrators) is compromised, data are partially distorted, but the situation remains manageable through local response measures.

S_2 – Large-scale compromise: telemetry substitution and false notifications become systemic, creating risks of incorrect control commands and mismatches between generation and demand.

S_3 – Functional failure: complete loss of data integrity renders control impossible; the consequences are comparable to a large-scale "data-driven blackout."

Formalization of State Transitions

Transitions between states are described by transition rates (measured in [1/hour]), which depend on the attack frequency (λ), the probability of successful compromise (p_c), the coefficients of cascading propagation (γ_1, γ_2), as well as recovery parameters (μ_1, μ_2, ρ_0, ρ_1). In addition, the model incorporates the detection rate (δ).

Transition formulas:

Compromise: $a_{01}=\lambda p_c a$, $a_{12}=\lambda p_c \cdot k_{12}$, $a_{23}=\lambda p_c \cdot k_{23}$

Cascading effects: $S_1 \rightarrow S_2 : \gamma_1$, $S_2 \rightarrow S_3 : \gamma_2$

Recovery: $S_1 \rightarrow S_0 : \mu_1$, $S_2 \rightarrow S_1 : \mu_2$, $S_3 \rightarrow S_2 : \rho$

4 Mathematical Formulation

The system dynamics are described by the CTMC generator Q, where each diagonal component equals the negative sum of the outgoing transition rates.

Initial probability distribution: $p(0)=[1,0,0,0]$.

Time evolution: $p(t)=p(0)e^{Qt}$.

Stationary distribution: $\pi Q=0$.

5 Calculated Indicators

Based on the model, several key resilience metrics are defined:

Probability of functional failure at time t: $P_{BL}(t)=p_3(t)$

Data Integrity Loss (DIL) – the expected fraction of unreliable data:

$DIL(t)=p(t) \cdot w^{\top}$, $w=[0,w_1,w_2,w_3]$, $w_3=1$.

Mean Time to Detection (MTTD) and Mean Time to Recovery (MTTR) – average times of attack detection and system restoration.

Expected Unserved Energy (EUE-analogue) – the expected impact of corrupted data on power supply (1):

$EUE = \sum_{i=0}^{3} c_i\, p_i(t)$ (1)

where c_i – are the energy loss coefficients for each state.

Thus, the CTMC model formalizes not only the probabilities of transitions between Smart Grid states but also makes it possible to calculate integral resilience indicators, linking the dynamics of cyberattacks with their socio-economic consequences.

6 Risk Scenarios

The proposed model makes it possible to analyze various attack scenarios:

Frequent low-impact attacks – do not lead to severe consequences but impose a constant load on monitoring and response subsystems, causing an increase in false alarms.

Rare but targeted campaigns – have a high probability of rapid escalation to states S_2–S_3; in this case, detection and recovery speed become the key resilience factors.

Hybrid attacks (technical + social engineering) – simultaneously increase both the probability of successful penetration and the cascading coefficients (γ_1, γ_2), which significantly raises the risk of a systemic crisis.

Exploitation of asynchronous notifications – even a local compromise may escalate into a crisis situation due to the injection of false messages and incorrect operator responses.

7 Discussion

The results of simulation experiments show that two factors have the greatest impact on Smart Grid cyber resilience: the speed of attack detection and the efficiency of recovery. These factors determine the likelihood of local incidents escalating into systemic failures, as well as the level of economic damage inflicted on energy infrastructure.

Thus, the application of CTMC modeling not only provides a formalization of cyber threat dynamics but also creates tools for justifying investment decisions in cybersecurity, which is particularly important under the necessity of balancing innovation, costs, and resilience (A. P. Rozhenko., 2010).

8 Economic Dimension of Cyber Resilience

In addition to technical resilience, the proposed model also makes it possible to evaluate the economic efficiency of investments in cybersecurity. The analysis results indicate the existence of a critical investment range within which expenditures on protective measures significantly reduce the expected damage (E. B. Belov *et al.,* 2006). Beyond this range, however, further budget increases demonstrate a diminishing returns effect: higher costs are accompanied by only marginal reductions in risk. This outcome is particularly important for strategic planning, as it helps to avoid both underinvestment, which leads to high vulnerability, and overspending, which fails to deliver proportional benefits.

9 Integration of Stochastic Modeling and Economic Analysis

The integration of stochastic modeling with methods of economic analysis enhances decision-making capabilities in energy companies and regulatory bodies. The proposed approach provides:

- justification of corporate cybersecurity strategies focused on efficiency;
- support for government regulators in adapting legal frameworks and standards to the conditions of energy digitalization;
- optimization of budget allocation aimed at protecting critical infrastructure.

Thus, economic cybernetics and mathematical modeling together form a unified toolkit that makes it possible to combine technical and managerial aspects.

10 Results and Discussion

The application of the model has made it possible to achieve the following results:

- formalization of cyber threats in probabilistic terms, enabling a shift from descriptive scenarios to quantitative assessments;

- prediction of incident dynamics and cascading effects, including the escalation of local attacks into systemic crises;
- resilience assessment based on key metrics such as DIL, MTTR, MTTD, and the EUE analogue, which link technical failures with socio-economic consequences;
- identification of optimal investment strategies in protective measures, allowing risk reduction while ensuring rational use of resources.

The final findings demonstrate that the combination of economic cybernetics principles and stochastic analysis forms a methodology that enables a balance between innovation, cost, and the resilience of energy infrastructure.

References

1. Belov, E.B., Los, V.P., Meshcheryakov, R.V. and Shelupanov, A.A. (2006) Fundamentals of information security. Moscow: Goryachaya Liniya - Telekom.
2. Fang, X., Misra, S., Xue, G. and Yang, D. (2012) 'Smart grid – The new and improved power grid: A survey', IEEE Communications Surveys & Tutorials, 14(4), pp. 944–980.
3. He, H. and Yan, J. (2016) 'Cyber-physical attacks and defenses in the smart grid: A survey', IEEE Transactions on Smart Grid, 7(1), pp. 281–299.
4. Metke, A.R. and Ekl, R.L. (2010) 'Security technology for smart grid networks', IEEE Transactions on Smart Grid, 1(1), pp. 99–107.
5. Mo, Y., Kim, T.H.-J., Brancik, K., Dickinson, D., Lee, H., Perrig, A. and Sinopoli, B. (2012) 'Cyber-physical security of a smart grid infrastructure', Proceedings of the IEEE, 100(1), pp. 195–209.
6. Rozhenko, A.P. (2010) Internal threats to the security of confidential information: Methodology and theoretical research. Moscow: Krasand.
7. Shcheglov, K.A. and Shcheglov, A.Yu. (2012) 'Protection against malicious software by controlling access to created file objects', Herald of Computer and Information Technologies, (8), pp. 46–51.
8. Shcheglov, K.A. and Shcheglov, A.Yu. (2014a) 'Mathematical models of operational information security', Information Protection Issues, 106(3), pp. 52–65.
9. Shcheglov, K.A. and Shcheglov, A.Yu. (2014b) 'Operational characteristics of information system security risks', Scientific and Technical Journal of Information Technologies, Mechanics and Optics, (1(89)), pp. 129–139.
10. Yan, Y., Qian, Y., Sharif, H. and Tipper, D. (2012) 'A survey on cyber security for smart grid communications', IEEE Communications Surveys & Tutorials, 14(4), pp. 998–1010.