

Article

Not peer-reviewed version

The Identification, Definition, Types and Propagation of the Instability and Insecurity Elements from Romanian Power System

Muresan-Grecu Florin , [Moraru Roland Iosif](#) , [Fiță Nicolae Daniel](#) ^{*} , Schiopu Adrian Mihai ,
Popescu Stelea Mihai , [Cruceru Alin Emanuel](#) , Sima Ioan , [Mila Ilieva Obretenova](#)

Posted Date: 31 March 2025

doi: 10.20944/preprints202503.2246.v1

Keywords: dysfunction; deficiency; non-compliance; vulnerability; risk; threat; hazard; aggression



Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Article

The Identification, Definition, Types and Propagation of the Instability and Insecurity Elements from Romanian Power System

Muresan-Grecu Florin ¹, Moraru Roland Iosif ¹, Fiță Nicolae Daniel ^{1,*}, Schiopu Adrian Mihai ¹, Popescu-Stelea Mihai ¹, Cruceru Emanuel Alin ², Sima Ioan ¹ and Mila Ilieva Obretenova ³

¹ University of Petrosani, Romania; flomavon2002@yahoo.com (MGF), roland_moraru@yahoo.com (MRI), daniel.fita@yahoo.com (FND), schiopu.adrian.mihai@gmail.com (SAM), popescusteleamihai@yahoo.ro (PSM), simaioan@yahoo.com (SI)

² University Politehnica of Bucharest, Romania; alincruceru1988@gmail.com

³ University of Mining and Geology St. Ivan Rilski Sofia, Bulgaria; mila.ilieva@mgu.bg

* Correspondence: daniel.fita@yahoo.com

Abstract: A adaptable, resilient, safe and secure power system is essential for ensuring energy and national security, having a direct impact on a state's economy, social stability, and well-being through the following requirements: Ensuring continuity of power supply (a robust power system guarantees uninterrupted access to electricity for citizens, institutions, and industries, reducing the risk of disruptions caused by technical deficiencies, cyberattacks, or geopolitical instability); Energy independence and reduction of external dependence (a state that produces sufficient electricity from its own sources is less vulnerable to international market fluctuations and external pressures, while diversifying energy sources—renewable, nuclear, hydrocarbons—reduces import dependence and economic vulnerability); Security of power infrastructure (protecting electricity networks from physical and cyberattacks is essential for the normal functioning of society, and developing modern infrastructure—smart grids, electricity storage—ensures the resilience of the energy system); Economic stability and national development (an efficient power system supports industry, agriculture, and services, contributing to economic growth, while lower energy costs enhance economic competitiveness and attract investments); Environmental protection and energy transition (adopting renewable sources and clean technologies reduces dependence on fossil fuels and minimizes environmental impact, while increasing energy efficiency and reducing carbon emissions are essential for long-term sustainability); Strategic and geopolitical role (countries with significant energy resources have greater influence on the international stage, and regional energy cooperation can strengthen diplomatic and economic relations). A secure and efficient energy system is the backbone of national security, guaranteeing economic stability, strategic independence, and population protection. Investments in modern infrastructure, clean technologies, and diversification of energy sources are crucial for the energy future of any nation. The authors of this study have identified all elements of instability and insecurity within Romania's Power System, with the aim of evaluating them and subsequently developing safety and security strategies.

Keywords: dysfunction; deficiency; non-compliance; vulnerability; risk; threat; hazard; aggression

1. Introduction

A. Essential information regarding National Power System (Figure 1):

Romania is integrated into the European electricity transmission network, part of the European Network of Transmission System Operators for Electricity (ENTSO-E). International interconnections enable energy exchanges, optimisation of energy resources and contribute to system stability in the event of major variations in consumption or production. The structure of the National Power System

is the set of interconnected components that ensure the production, transmission, distribution and consumption of electricity. Electricity production in Romania is based on a combination of energy sources, and the energy landscape of the country has evolved over time, based on conventional and renewable energy sources. Romania has a diversified energy infrastructure, with power plants that use several energy sources, including nuclear energy, hydropower, fossil fuel energy (lignite, hard coal, natural gas) and renewable energy (wind, solar, biomass). Electricity transmission is carried out through the National Power Grid, which plays a key role in the transmission of electricity from producers to distributors and is responsible for the safety and reliability of the National Power System. The structure of the power grid includes very and high voltage overhead power lines, power substations and dispatching. The power infrastructure is composed of 81 power substations, of which 1 power substation at 750 kV (working at 400 kV), 38 power substation at 400 kV and 42 power substations at 220 kV. The distribution of electricity is carried out through the Power Distribution Network, which is an essential part of the national power infrastructure, responsible for the distribution of electricity to consumers. This network includes overhead power lines and power substations at 110 kV providing power to both urban and rural areas [1,2].

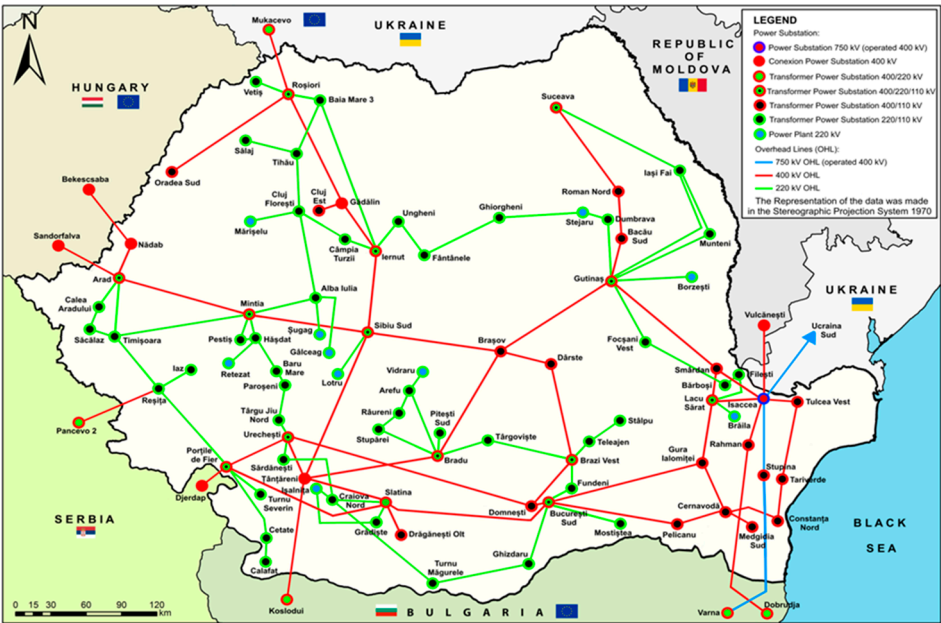


Figure 1. National Power System map.

B. The importance of the study in the context of ensuring energy security: [3]

The essential purpose of this paper is to identify all the elements of instability and insecurity to critical infrastructures within The National Power System, by next actions:

- identifies the possible systemic dysfunctions, deficiencies and non-compliances;
- identifies the possible vulnerabilities originated from systemic dysfunctions, deficiencies and non-compliances;
- identifies the possible risks originated from vulnerabilities;
- identifies the possible threats originated from risks ;
- identifies the possible hazards originated from threats;
- identifies the possible aggressions originated from dangers.

Knowing all the instability and insecurity elements the following actions can be carried out:

- the assessment of the vulnerabilities;
- the assessment of the risks;
- the assessment of the threats;
- the assessment of the hazards;

- the assessment of the agressions.

Following the assessment of the vulnerabilities, risks, threats, hazards and aggressions, the following actions can be carried out:

- assessment of the security state of The National Power System;
- development of the security strategies of The National Power System.

Types of national security strategies:

(a) The national strategy of security and protection of the critical infrastructures within the National Power System:

- power plants for producing electricity;
- power substations for transmission of electricity;
- overhead power lines for transmission of electricity.

(b) The national strategy of power safety focused on The National Power System:

- power plants for producing electricity;
- power substations for transmission of electricity;
- overhead power lines for transmission of electricity.

Because The National Power System is vulnerable, it can be, at any time, the target of terrorist threats or attacks (bomb or cyber attacks), natural risks (calamities caused by nature) and anthropic risks (caused by man), which could endanger the proper functioning, or in the most unfortunate case, its total outage – black-out, generating a major crisis that could cause extreme damage to the citizen, society and state.

The National Power System is the generator of critical infrastructures (power plants, power substations and overhead power lines), because it ensures the health and safety of the citizens by supplying all of the state systems, the industry and the national economy with electricity and has a substantial contribution to ensuring national security and well-being, as shown in Figure 2 [4].

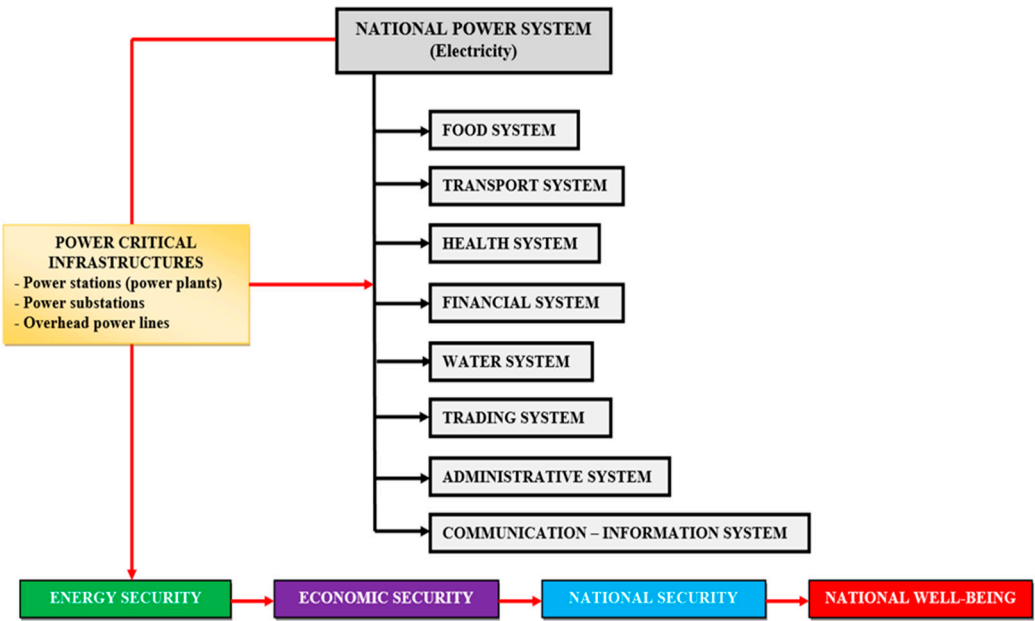


Figure 2. The dependence of state systems, economy and national industry on electricity.

C. The risk analysis – Quantitative risk matrix on 5 levels: [5]

Defining likelihood and impact levels:

A. Likelihood (L):

- 1: Very low;
- 2: Low;

- 3: Medium;
- 4: High;
- 5: Very high.

B. Impact (I):

- 1: Very low;
- 2: Low;
- 3: Medium;
- 4: High;
- 5: Very high.

Building the risk matrix:

$$FR = P \cdot I \quad (1)$$

where:

$$P = [5 \ 4 \ 3 \ 2 \ 1]^T;$$

$$I = [1 \ 2 \ 3 \ 4 \ 5]$$

Following the calculations, we get:

$$FR = \begin{bmatrix} 5 & 10 & 15 & 20 & 25 \\ 4 & 8 & 12 & 16 & 20 \\ 3 & 6 & 9 & 12 & 15 \\ 2 & 4 & 6 & 8 & 10 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}$$

The classification of the risks:

The risks shall be classified according to the FR value obtained:

- FR between 1 and 3: Very low risk;
- FR between 4 and 6: Low risk;
- FR between 7 and 12: Medium risk;
- FR between 13 and 16: High risk;
- FR between 17 and 25: Very high risk.

Example: Suppose we have a risk with:

- medium likelihood: 3;
- high impact: 4;
- $FR = 3 \cdot 4 = 12$;
- medium risk level: 12.

This matrix model allows for a clear and structured risk assessment, facilitating their identification and effective management.

The residual risk calculation:

Residual risk (RR) is the remaining risk after applying the control factors.

The control factors are used to reduce the risk.

These factors may include preventive, detector, and corrective measures.

Each control factor has an efficiency (E) between 0 and 1, where 1 means maximum efficiency.

$$RR = FR \cdot (1 - E) \quad (2)$$

Example: Suppose we have a risk with:

- medium likelihood: 3;
- high impact: 4;
- control factor with 0.7 efficiency.

Then:

$$FR = 3 \cdot 4 = 12$$
$$RR = 12 \cdot (1 - 0.7) = 3.6$$

The assessment of the combined risk:

For multiple risks, we evaluate the combined risk (CR) using an aggregation method, such as the weighted amounts of individual risks:

$$RC = \sum_i (FR_i \cdot W_i)$$

(3)

where:

- (FR_i) is the risk factor for the risk i;
- (W_i) is the weight assigned to risk i.

Note:

To develop previous relationships, a risk factor must be identified.

The identification of risk factors relevant to the specific context (for example, environmental, financial, operational, technological risk, etc.).

2. State of Art – Recent Evolution

Identifying the instability and insecurity elements (dysfunction, deficiencies, non-compliances, vulnerabilities, risks, threats, hazards and aggression) of a power system is crucial to ensuring energy security, reducing risks and promoting sustainability. Here are some main reasons why this analysis is crucial: Ensuring Energy Security (the vulnerabilities of an power system can lead to power supply disruptions, affecting the economy and quality of life, while identifying weak points allows for the development of resilience strategies), Managing Geopolitical Risks (electricity is often used as a geopolitical tool, and excessive dependence on fossil fuel imports from certain regions can expose states to major risks in the event of international conflicts or economic sanctions), Adapting to Climate Change (climate change affects power infrastructure through extreme weather events, and assessing vulnerabilities enables the development of adaptation solutions and investments in renewable sources), Protection Against Cyber and Physical Attacks (power systems are increasingly digitalized, making them vulnerable to cyberattacks; additionally, physical infrastructure: power stations and high-voltage overhead and underground power lines, can be targeted by terrorist attacks or sabotage), Ensuring Equitable Access to Energy (many regions of the world still lack stable access to electricity, and identifying vulnerabilities helps in developing effective electrification and economic development policies), Stabilizing Energy Markets and Preventing Economic Crises (electricity prices are influenced by the vulnerabilities of power systems, and energy crises can destabilize entire economies, making continuous risk analysis essential), Developing Resilient and Sustainable Energy Systems (identifying vulnerabilities helps build flexible systems based on energy source diversification, energy storage, and the development of smart grids). The analysis of instability and insecurity elements within an power system is essential for ensuring energy security, economic stability, and environmental protection. It allows for the identification of risks, threats, hazards, and aggressions that may affect energy supply and provides solutions to mitigate their impact [6–31].

Worldwide research on the insecurity and instability of power systems, as well as the analysis and identification of vulnerabilities, risks, dangers and aggressions on them, are summarized:

Specialists	Entity	Paper
Banghua Xie, Xiaoge Tian, Liulin Kong, Weiming Chen	Faculty of Engineering, China University of Geosciences, Wuhan, Chia	The vulnerability of the power grid structure: a system analysis based on complex network theory
Francesco Cadini, Luca Lomazzi, Enrico Zio	Politecnico di Milano and Centre for Research on Risk and Crises, Paris	Vulnerability analysis of power transmission grid subject to cascading failures

Ersen Akdeniz, Mustafa Bagriyanik	Istanbul Technical University, Istanbul, Turkey, Siemens Gamesa Renewable Enerji, Izmir, Turkey	A preventive control approach for power system vulnerability assessment and predictive stability evaluation
Tianlei Zang, Zian Wang, Xiaoguang Wei, Yi Zhou, Jiale Wu, Buxiang Zhou	Sichuan University, Chengdu, China, Southwest Jiaotong University, Chendu, China	Current status and perspective of vulnerability assessmeny of cyber-physical power system based on complex network theory
Nikolaos Nikolaou, Abdreas Papadakis, Konstantinos Psychogyios, Theodore Zahariadis	Sunelixis Solution, Chalkida, Greece, School of Pedagogical and Technological Education, Athens, Greece, National and Kapodistrian University of Athens, Greece	Vulnerability identification and assessmeny for critical infrastructures in energy sector
Jun Guo, Tao Feng, Zelin Cai, Xiaolong Lian, Wenhui Tang	State Key Laboratory of Disaster Prevention and Reduction for Power Grid Transmission and Distribution Equipment, Changsha, China, School of Electric Power Engineering, South Chia University of Technology, Guanzhou, China	Vulnerability assessment for power transmission lines under typhoon weather base on a cascading failure state transition diagram
Yu-Shuai Li, Da-Zhong Ma, Hua-Guang Zhang, Qie-Ye Sun	Northeastern University, Shenyang, China	Critical nodes identification of power systems based on controllability of complex networks

3. Identification and Definition of the Instability and Insecurity Elements

3.1. Identification

The following instability and insecurity elements are identified for critical infrastructures within The National Power System, through The Power Transmission Grid, as shown in Figure 3: [29]

- (a) Systemic elements:
- dysfunctions;
 - deficiencies;
 - non-compliances.
- (a) Vulnerabilities;
- (b) Risks;
- (c) Threats;
- (d) Hazards;
- (e) Agressions.

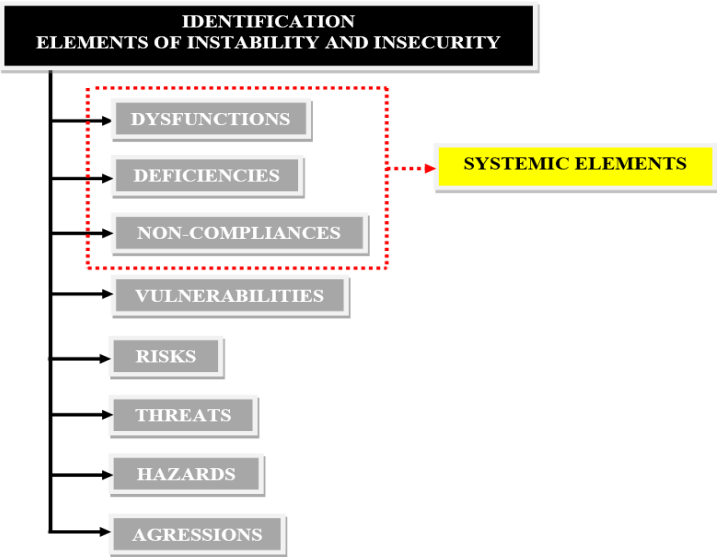


Figure 3. The identification of instability and insecurity elements.

3.2. Definition

A. Systemic elements

- a) Dysfunctions: The dysfunctions are those actions manifested by failures and/or disturbances of the functions of a system, with the effect of reducing, integrating or adapting of critical infrastructure, and the unidentification, superficial treatment or poor management of the dysfunctions automatically generates vulnerabilities, which can affect the smooth running of the critical infrastructure.
- b) Deficiencies: The deficiencies represents the lack of physical attributes manifested by defects or gaps and are characterized by deficiency, and a critical infrastructure with deficiencies cannot operate at its normal parameters and urgent re-commissioning or resilience measures must be taken.
- c) Non-compliances: The non-compliances represents the failure to meet the requirements of a critical infrastructure, manifested by the deviation of some characteristics from the requirements specified in the security plan or operating manual, and a critical infrastructure with non- compliances cannot operate at its normal parameters and urgent measures must be taken to eliminate non-compliances.

B. Vulnerabilities

The vulnerabilities generated by systemic dysfunctions, deficiencies or non-compliances are factual states, processes and phenomena that diminish the responsiveness of critical infrastructures to potential risks or threats or that favor their emergence and development, with consequences in terms of functionality and utility. Non-knowledge, non-management or poor and faulty management of vulnerabilities may result in risk factors, threats, dangers or aggression towards national objectives, values, interests and needs subsumed to critical infrastructures.

C. Risks

The risks generated by certain vulnerabilities, designate situations, circumstances, elements or internal or external conjunctions, sometimes doubled and operative, which determine or favor the materialization of a threat to critical infrastructure, generating insecurity effects.

D. Threats

The threats generated by risk factors are capacities, strategies, intentions, plans that potentiate a danger to critical infrastructures, materialized by attitudes, gestures, acts, facts that create states of imbalance or instability and generate states of hazard, with impact on security.

E. Hazards

The hazards arising from certain threats are situations, events that can endanger or threaten the existence or integrity of critical infrastructures.

F. Agressions

The aggressions arising from certain danger condtions are attacks, including armed attacks, which jeopardize the existence, balance or integrity of critical infrastructures.

4. Types of the Instability and Insecurity Elements from Romanian Power System

A. Types of systemic elements

- a) Dysfunctions: dysfunctions identified within The National Power System, as shown in Table 1: [1–4].

Table 1. Dysfunctions identified within The National Power System.

THE IDENTIFIED DYSFUNCTION	THE GENERATED VULNERABILITY
1. Lack, precariousness or non-compliance with the activities of exploitation, maintenance and development of The Power Transmission Grid: • lack, precariousness or non-compliance with exploitation procedures;	1. Poor management of the transmission operator activity (exploitation, maintenance and development) of The Power Transmission Grid installations.

• lack, precariousness or non-compliance with maintenance procedures; • lack, precariousness or non-compliance with development procedures.	
2. Lack, precariousness or non-compliance with the activities of operative and operational management of The National Power System: • lack, precariousness or non-compliance with dispatching procedures; • lack or precariousness of investments in EMS/SCADA of The National Power System). • lack, precariousness or non-compliance with cyber security procedures.	
3. Lack or precariousness of investments in the infrastructure of The Power Transmission Grid	2. Poor management of the system operator activity (operative and operational management) 3. Instability and insecurity of The National Energy System caused by lack or precarious investments in the power infrastructure.
4. Lack, precariousness or non-compliance with the cyber security activity within The National Power System: • lack, precariousness or non-compliance with cyber security procedures; • underperforming EMS/SCADA infrastructure.	
5. Lack, precariousness or non-compliance with Occupational Health and Safety activity within the jobs: • lack, precariousness or non-compliance with Occupational Health and Safety procedures; • lack, precariousness or non-compliance with the electrical safety procedures; • lack, precariousness or non-compliance with the evaluation and audit in terms of Occupational Health and Safety; • lack, precariousness or non-compliance with the Prevention and Protection Plan.	
6. Lack, precariousness or non-compliance with the activity of protection and security of critical infrastructures within The National Power System: • lack, precariousness or non-compliance with Critical Infrastructure Protection procedures; • lack, precariousness or non-compliance with the Security Plan at the Operator; • lack, precariousness or non-compliance with physical security procedures; • lack, precariousness or non-compliance with the strategy for the protection of national and european critical infrastructure on The Power Transmission Grid.	
7. Lack, precariousness or non-compliance with development strategies and safety and security strategies within The National Power System: • lack, precariousness or non-compliance with the development strategy on The Power Transmission Grid; • lack, precariousness or non-compliance with the strategy of protection and security of critical infrastructures within The National Power System; • lack, precariousness or non-compliance with the power safety strategy of The National Power System	
4. The precariousness of Cyber Security activity. 5. The precariousness of Occupational Health and Safety activity. 6. The precariousness of the protection and security activity of critical infrastructures 7. Lack of strategies for the development of The Power Transmission Grid, critical infrastructure protection and cyber security of The National Power System	

b) Deficiencies: deficiencies identified within The National Power System, as shown in Table 2: [1–4].

Table 2. Deficiencies identified within The National Power System.

THE IDENTIFIED DEFICIENCY	THE GENERATED VULNERABILITY
1. Removing coal-fired capacities from production and increasing consumption through energetic aid provided for the Republic of Moldova and Ukraine	1. Power deficit in The National Power System.

2. Acquisition of electricity produced from renewable resources	2. Deficit regarding the capacity of The National Power System.
3. A number of installations for the production, transmission and distribution of electricity are obsolete and technologically outdated, with high consumption and operating costs, causing very frequent defects, disturbances and damages.	3. Deficit of high-performance energetic installations in The Power Transmission Grid
4. Energy prices do not reflect the security of energy supply depending on the position of the consumer/producer in the load curve.	4. Deficit of incentives for investments in top-notch capacities.
5. Lack of electricity storage elements	5. Deficit of electricity storage infrastructures.
6. Lack of infrastructure for closing the 400 kV ring	6. Non-closure of the 400 kV ring in the N and S-W area of Romania.
7. Lack of financial measures to support projects and programs of increasing energetic efficiency and lack of european funds for investments in modern energetic infrastructure.	7. Deficit of financial resources
8. Reduced research-development-dissemination capacity in the energetic and mining sector	8. Deficit of research-development resources.
9. The intervention of the political factor or nepotism within the transport company (top management, territorial transport units, exploitation centers, power substations and dispatchers).	9. Deficit of qualified and overqualified human resource.
10. Possible thefts and sabotage from own facilities	10. Deficit of honest and serious human resources.
11. Political and legislative unpredictability	11. Deficit of political and legislative stability.

c) Non-compliances: non-compliances identified within The National Power System, as shown in Table 3: [1–4].

Table 3. Non-compliances identified within The National Power System.

THE IDENTIFIED NON-COMPLIANCE	THE GENERATED VULNERABILITY
1. Unexpected disconnection of protection equipment and devices within power substations.	1. Precariousness and non-performance of energetic equipment and appliances within The Power Transmission Grid
2. Poor condition of energetic equipment and appliances	2. Lack of electricity – possible local, area, regional or national blackout.
3. Lack of electricity from national systems.	3. The dependence of national systems on electricity.

B. Types of vulnerabilities

The vulnerabilities identified caused by systemic elements (dysfunctions, deficiencies and non-compliances) within The National Power System are the following, as shown in Table 4: [1–4].

Table 4. Vulnerabilities identified within The National Power System.

No.	THE IDENTIFIED VULNERABILITY	GENERATING SOURCE
1.	Poor management of the transmission operator activity (exploitation, maintenance and development) of The Power Transmission Grid installations.	Dysfunction of The National Power System
2.	Poor management of the system operator activity (operative and operational management) of The National Power System).	
3.	Instability and insecurity of The National Power System caused by lack or precarious investments in the power infrastructure.	
4.	The precariousness of Cyber Security activity.	
5.	The precariousness of Occupational Health and Safety activity.	
6.	The precariousness of the protection and security activity of critical infrastructures.	
7.	Lack of strategies for the development of The Power Transmission Grid, critical infrastructure protection and cyber security of The National Power System.	Deficiency of The National Power System
8.	Power deficit in The National Power System.	
9.	Deficit regarding the capacity of The National Power System	
10.	Deficit of high-performance energetic installations in The Power Transmission Grid installations.	

11.	Deficit of incentives for investments in top-notch capacities.	
12.	Deficit of electricity storage infrastructures	
13.	Non-closure of the 400 kV ring in the N and S-W area of Romania.	
14.	Deficit of financial resources.	
15.	Deficit of research-development resources.	
16.	Deficit of qualified and overqualified human resource.	
17.	Deficit of honest and serious human resources.	
18.	Deficit of political and legislative stability.	
19.	Precariousness and non-performance of energetic equipment and appliances within The Power Transmission Grid.	Non-compliance of The National Power System
20.	Lack of electricity – possible local, area, regional or national black-out.	
21.	The dependence of national systems on electricity.	

C. Types of risks

The risks identified caused by vulnerabilities within The National Power System are the following, as shown in Table 5: [1–4].

Table 5. Identified risks within The National Power System.

No.	THE IDENTIFIED RISK	THE GENERATING VULNERABILITY
1.	Risk of technical incident (isolated/associated), technical disturbance or damage.	Poor management of the transmission operator activity (exploitation, maintenance and development) of The Power Transmission Grid installations.
2.	Risk of operative and/or operational incident	Poor management of the system operator activity (operative and operational management) of The National Power System).
3.	Risk of partial or total disconnection of The National Power System – black-out	Instability and insecurity of The National Energy System caused by lack or precarious investments in the power infrastructure.
4.	Risk of cyber attack	The precariousness of Cyber Security activity.
5.	Risk of injury (electrocution) and/or occupational illness.	The precariousness of Occupational Health and Safety activity.
6.	Risk of terrorist attack	The precariousness of the protection and security activity of critical infrastructures
7.	Risk of partial or total black-out of The National Power System	Lack of strategies for the development of The Power Transmission Grid, critical infrastructure protection and cyber security of The National Power System
8.	Risk of power shortage and purchasing import electricity → the unprofitability of The National Power System.	Power deficit in The National Power System.
9.	Risk of non-symmetric and un-equilibrated charging of electricity → partial or total disconnection of The National Power System – black-out.	Deficit regarding the capacity of The National Power System.
10.	Major risk of associated technical incident and technical damage → black-out.	Deficit of high-performance energetic installations in The Power Transmission Grid installations.
11.	Risk of energetic insecurity.	Deficit of incentives for investments in top-notch capacities.
12.	Risk of energetic insecurity.	Deficit of electricity storage infrastructures.
13.	Risk of partial or total disconnection of The National Power System – black-out	Non-closure of the 400 kV ring in the N and S-W area of Romania.
14.	Financial risk	Deficit of financial resources
15.	Risk of deficit research-development	Deficit of research-development resources.
16.	Risk of shortage of skilled and overqualified human resources → mistakes of the management, operative and dispatching staff → black-out.	Deficit of qualified and overqualified human resource.
17.	Risk of sabotage.	Deficit of honest and serious human resources.
18.	Political and legislative risk	Deficit of political and legislative stability.
19.	Risk of unexpected disconnection → partial or total black-out	Precariousness and non-performance of energetic equipment and appliances within The Power Transmission Grid
20.	Risk of energetic crisis.	Lack of electricity – possible local, area, regional or national black-out.

21.	Risk of energetic crisis→national crisis→national insecurity→collapse	The dependence of national systems on electricity.
-----	---	--

D. Types of threats

Identified threats caused by risks within The National Power System are the following, as shown in Table 6: [1–4].

Table 6. Identified threats within The National Power System.

No.	THE IDENTIFIED THREAT	THE GENERATING RISK
1.	Technological threat.	Risk of technical incident (isolated/associated), technical disturbance or damage.
2.	Operative and operational threat	Risk of operative and/or operational incident
3.	Threat of energetic crisis.	Risk of partial or total disconnection of The National Power System – black-out.
4.	Cyber (terrorist) threat.	Risk of cyber attack.
5.	Threat of death.	Risk of injury (electrocution) and/or occupational illness.
6.	Terrorist threat.	Risk of terrorist attack.
7.	Threat of energetic crisis.	Risk of partial or total black-out of The National Power System.
8.	Economic threat	Risk of power shortage and purchasing import electricity → the unprofitability of The National Power System.
9.	Threat of energetic crisis.	Risk of non-symmetric and un-equilibrated charging of electricity → partial or total disconnection of The National Power System – black-out.
10.	Threat of energetic crisis.	Major risk of associated technical incident and technical damage → black-out.
11.	Threat of energetic crisis.	Risk of energetic insecurity.
12.	Threat of energetic crisis.	Risk of energetic insecurity.
13.	Threat of energetic crisis.	Risk of partial or total disconnection of The National Power System – black-out
14.	Financial threat.	Financial risk
15.	Threat of research-development crisis.	Risk of deficit research-development
16.	Threat of qualified and overqualified staff crisis.	Risk of shortage of skilled and overqualified human resources → mistakes of the management, operative and dispatching staff → black-out.
17.	Threat of sabotage.	Risk of sabotage.
18.	Political and legislative threat.	Political and legislative risk
19.	Threat of energetic crisis.	Risk of unexpected disconnection→ partial or total black-out
20.	Threat of national collapse.	Risk of energetic crisis
21.	Threat of national collapse.	Risk of energetic crisis→national crisis→national insecurity→collapse

Other identified threats naturally caused with a crisis or collapse effect on The National Power System, as shown in Table 7: [1–4].

Table 7. Identified threats from the outside with effect on The National Power System.

No.	THE IDENTIFIED THREAT	THE GENERATING RISK
Threat of natural disaster:		
1.	(a) earthquake;	Natural risk
	(b) hurricane;	
	(c) flood;	
	(d) volcano;	
	(e) landslide;	
	(f) drought;	
	(g) meteor strike;	
	(h) solar storm, etc.	

E. Types of hazards

Identified hazards caused by threats within The National Power System are the following, as shown in Table 8: [1–4].

Table 8. Identified dangers within The National Power System.

No.	THE IDENTIFIED HAZARDS	THE GENERATING THREAT
1.	Hazard of technological instability (incident/damage) → black-out.	Technological threat.
2.	Hazard of operative and operational insecurity→ black-out.	Operative and operational threat
3.	Hazard of national insecurity → lack of national welfare	Threat of energetic crisis.
4.	Hazard of cyber insecurity → black-out.	Cyber (terrorist) threat.
5.	Hazard of human insecurity (work accident).	Threat of death.
6.	Terrorist Hazard → black-out.	Terrorist threat.
7.	Hazard of energetic crisis → national insecurity.	Threat of energetic crisis.
8.	Hazard of energetic crisis → national insecurity.	Economic threat.
9.	Hazard of energetic crisis → national insecurity.	Threat of energetic crisis.
10.	Hazard of energetic crisis → national insecurity.	Threat of energetic crisis.
11.	Hazard of energetic crisis → national insecurity.	Threat of energetic crisis.
12.	Hazard of energetic crisis → national insecurity.	Threat of energetic crisis.
13.	Hazard of energetic crisis → national insecurity.	Threat of energetic crisis.
14.	Hazard of financial crisis → economic insecurity.	Financial threat.
15.	Hazard of research-development crisis → energetic insecurity	Threat of research-development crisis.
16.	Hazard of staff crisis → energetic insecurity	Threat of qualified and overqualified staff crisis.
17.	Hazard of sabotage → energetic insecurity	Threat of sabotage.
18.	Hazard of political and legislative crisis → national insecurity	Political and legislative threat.
19.	Hazard of energetic crisis → national insecurity.	Threat of energetic crisis.
20.	Hazard of national collapse → lack of national welfare	Threat of national collapse.
21.	Hazard of national collapse → lack of national welfare	Threat of national collapse.

Other identified hazards naturally caused with a crisis or collapse effect on The National Power System, as shown in Table 9: [1–4].

Table 9. Identified dangers from the outside with effect on The National Power System.

No.	THE IDENTIFIED HAZARD	THE GENERATING THREAT
		Threat of natural disaster:
		(a) earthquake;
		(b) hurricane;
		(c) flood;
1.	Hazard of natural disaster.	(d) volcano;
		(e) landslide;
		(f) drought;
		(g) meteor strike;
		(h) solar storm, etc.

F. Types of aggression

Identified aggression caused by dangers within The National Power System are the following, as shown in Table 10: [1–4].

Table 10. Identified aggressions within The National Power System.

No.	IDENTIFIED AGRESSIONS	THE GENERATING DANGER
1.	Cyber attack → black-out.	Danger of cyber insecurity → black-out.
2.	Physical attack.	Danger of human insecurity.
3.	Terrorist attack: armed/bomb → black-out.	Terrorist danger → black-out.
4.	Attack from the inside (theft/armed attack/cyber attack) → black-out	Danger of sabotage → energetic insecurity.

Other identified aggressions naturally caused with a crisis or collapse effect on The National Power System, as shown in Table 11: [1–4].

Table 11. Other identified aggressions with effect on The National Power System.

No.	THE IDENTIFIED AGRESSIONS	THE GENERATING DANGER
1.	Attacks caused by natural disasters.	Danger of natural disaster.

5. Propagation of the Instability and Insecurity Elements

Figure 4 shows the scheme of propagation of system, instability and insecurity elements, and Figure 5 shows the sequence (phases) of propagation. [1–4].

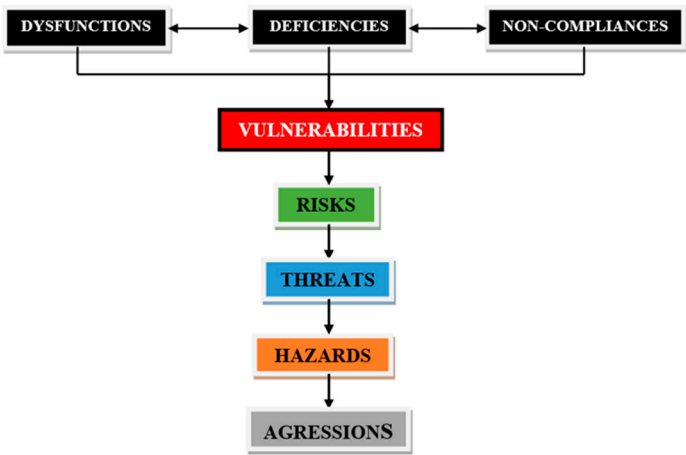


Figure 4. The scheme of propagation of system, instability and insecurity elements.

Phase 1: The identification and analysis of the systemic elements:

- dysfunctions;
- deficiencies;
- non-compliances;

Phase 2: The identification and assessment of vulnerabilities generated by systemic elements (dysfunctions, deficiencies and non-compliances);

Phase 3: The identification and assessment of risks generated by the identified vulnerabilities;

Phase 4: The identification and assessment of threats generated by the identified risks;

Phase 5: The identification and assessment of hazards generated by the identified threats;

Phase 6: The identification and assessment of the aggressions generated by the identified dangers;

Phase 7: The assessment of the security state of The National Power System;

Phase 8: The development of The National Power System security strategies.

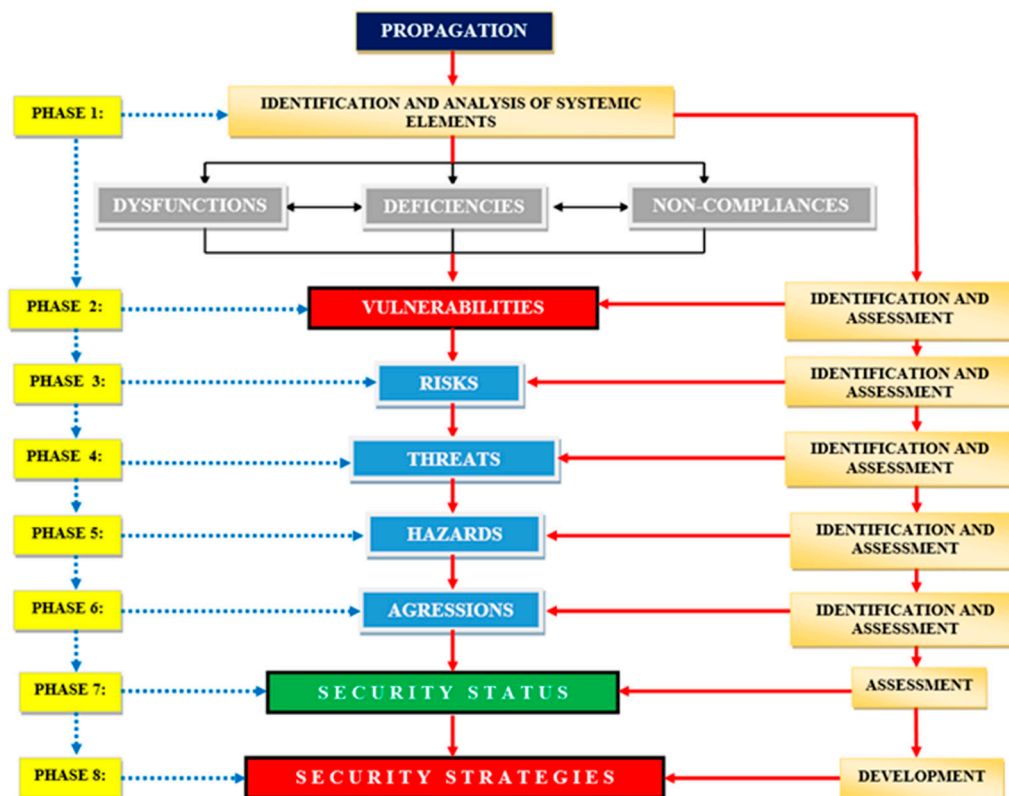


Figure 5. The sequence (phases) of propagation of system, instability and insecurity elements.

6. Prioritizing of the Instability and Insecurity Elements from Romanian Power System

6.1. Vulnerabilities

A. Estimating the Gravity: in this stage, the vulnerability gravity will be estimated:

Level	Gravity
1. Very low	The event produces a minor disturbance in the activity, without material damage
2. Low	The event causes minor material damage and limited disruption to activity
3. Medium	Injuries to staff, and/or certain losses of equipment, utilities and delays in providing the service.
4. High	Serious staff injuries, significant loss of equipment of installations and facilities, delays and/or interruption of service provision.
5. Very high	The consequences are catastrophic resulting in deaths and serious injuries to staff, major losses in equipment, installations and facilities and termination of service provision.

B. Estimating the Impact: in this stage, the vulnerability impact will be estimated:

Level	Impact
1. Very low	The event produces a minor disturbance in the activity, without material damage
2. Low	The event causes minor material damage and limited disruption to activity

3. Medium	Injuries to staff, and/or certain losses of equipment, utilities and delays in providing the service.
4. High	Serious staff injuries, significant loss of equipment of installations and facilities, delays and/or interruption of service provision.
5. Very high	The consequences are catastrophic resulting in deaths and serious injuries to staff, major losses in equipment, installations and facilities and termination of service provision.

C. Scenario type: after estimating the vulnerability gravity and impact, the type of scenario will be decided, according with Table 12:

- 1. The worst;
- 2. Plausible the worst;
- 3. Moderate.

1. The worst	2. Plausible the worst	3. Moderate

Table 12. Scenario type.

No.	THE IDENTIFIED VULNERABILITY (generated by dysfunction, deficiency and/or non-compliance)	ESTIMATING THE GRAVITY	ESTIMATING THE IMPACT	SCENARIO TYPE
1.	Poor management of the transmission operator activity (exploitation, maintenance and development) of The Power Transmission Grid installations.	5. Very high	5. Very high	1. The worst
2.	Poor management of the system operator activity (operative and operational management) of The National Power System).	4. High	4. High	2. Plausible the worst
3.	Instability and insecurity of The National Power System caused by lack or precarious investments in the power infrastructure.	5. Very high	5. Very high	1. The worst
4.	The precariousness of Cyber Security activity.	5. Very high	5. Very high	1. The worst
5.	The precariousness of Occupational Health and Safety activity.	4. High	4. High	3. Moderate
6.	The precariousness of the protection and security activity of critical infrastructures	5. Very high	5. Very high	2. Plausible the worst
7.	Lack of strategies for the development of The Power Transmission Grid, critical infrastructure protection and cyber security of The National Power System	3. Medium	3. Medium	3. Moderate
8.	Power deficit in The National Power System.	5. Very high	5. Very high	2. Plausible the worst
9.	Deficit regarding the capacity of The National Power System.	5. Very high	5. Very high	2. Plausible the worst
10.	Deficit of high-performance energetic installations in The Power Transmission Grid installations.	4. High	4. High	3. Moderate
11.	Deficit of incentives for investments in top-notch capacities.	4. High	4. High	3. Moderate
12.	Deficit of electricity storage infrastructures.	3. Medium	3. Medium	3. Moderate
13.	Non-closure of the 400 kV ring in the N and S-W area of Romania.	5. Very high	5. Very high	2. Plausible the worst
14.	Deficit of financial resources	4. High	4. High	3. Moderate
15.	Deficit of research-development resources	4. High	4. High	3. Moderate
16.	Deficit of qualified and overqualified human resource.	5. Very high	5. Very high	2. Plausible the worst
17.	Deficit of honest and serious human resources.	5. Very high	5. Very high	2. Plausible the worst
18.	Deficit of political and legislative stability.	4. High	4. High	3. Moderate
19.	Precariousness and non-performance of energetic equipment and appliances within The Power Transmission Grid	5. Very high	5. Very high	2. Plausible the worst
20.	Lack of electricity – possible local, area, regional or national black-out.	5. Very high	5. Very high	1. The worst
21.	The dependence of national systems on electricity.	5. Very high	5. Very high	1. The worst

6.2. Risks

A. Estimating the Likelihood: in this stage, the risk likelihood will be estimated:

Score level	The likelihood	Time
1. Very low	It has a very low likelihood of occurring. Normal measures are required to monitor the evolution of the event.	over 20 years
2. Low	The event has a low likelihood of occurring. Efforts are needed to reduce the likelihood and/or mitigate the impact produced.	16 – 20 years
3. Medium	The event has a significant likelihood of occurring. Significant efforts are needed to reduce the likelihood and/or mitigate the impact produced.	11 – 15 years
4. High	The event has a likelihood of occurring. Priority efforts are needed to reduce the likelihood and mitigate the impact produced.	6 – 10 years
5. Very high	The event is considered imminent. Immediate and extreme measures are required to protect the objective, evacuation to a safe location if the impact so requires.	1 – 5 years

B. Estimating the Gravity: in this stage, the risk gravity will be estimated:

Level	Gravity
1. Very low	The event produces a minor disturbance in the activity, without material damage
2. Low	The event causes minor material damage and limited disruption to activity
3. Medium	Injuries to staff, and/or certain losses of equipment, utilities and delays in providing the service.
4. High	Serious staff injuries, significant loss of equipment of installations and facilities, delays and/or interruption of service provision.
5. Very high	The consequences are catastrophic resulting in deaths and serious injuries to staff, major losses in equipment, installations and facilities and termination of service provision.

C. Scenario type: after estimating the likelihood and gravity, the type of scenario will be decided, according with Table 13:

- 1. The worst;
- 2. Plausible the worst;
- 3. Moderate.

1. The worst	2. Plausible the worst	3. Moderate

Table 13. Scenario type.

No.	THE IDENTIFIED RISK (generated by the vulnerability)	ESTIMATING THE LIKELIHOOD	ESTIMATING THE GRAVITY	SCENARIO TYPE
1.	Risk of technical incident (isolated/associated), technical disturbance or damage.	5. Very high	5. Very high	1. The worst

2. Risk of operative and/or operational incident	4. High	4. High	2. Plausible the worst
3. Risk of partial or total disconnection of The National Power System – black-out.	5. Very high	5. Very high	1. The worst
4. Risk of cyber attack.	5. Very high	5. Very high	1. The worst
5. Risk of injury (electrocution) and/or occupational illness.	4. High	4. High	3. Moderate
6. Risk of terrorist attack.	5. Very high	5. Very high	2. Plausible the worst
7. Risk of partial or total disconnection of The National Power System – black-out.	3. Medium	3. Medium	3. Moderate
8. Risk of power shortage and purchasing import electricity → the unprofitability of The National Power System.	5. Very high	5. Very high	2. Plausible the worst
9. Risk of non-symmetric and un-equilibrated charging of electricity → partial or total disconnection of The National Power System – black-out.	5. Very high	5. Very high	2. Plausible the worst
10. Major risk of associated technical incident and technical damage → black-out.	4. High	4. High	3. Moderate
11. Risk of energetic insecurity.	4. High	4. High	3. Moderate
12. Risk of energetic insecurity.	3. Medium	3. Medium	3. Moderate
13. Risk of partial or total disconnection of The National Power System – black-out.	5. Very high	5. Very high	2. Plausible the worst
14. Financial risk	4. High	4. High	3. Moderate
15. Risk of deficit research-development	4. High	4. High	3. Moderate
16. Risk of shortage of skilled and overqualified human resources → mistakes of the management, operative and dispatching staff → black-out.	5. Very high	5. Very high	2. Plausible the worst
17. Risk of sabotage.	5. Very high	5. Very high	2. Plausible the worst
18. Political and legislative risk	4. High	4. High	3. Moderate
19. Risk of unexpected disconnection→ partial or total black-out	5. Very high	5. Very high	2. Plausible the worst
20. Risk of energetic crisis	5. Very high	5. Very high	1. The worst
21. Risk of energetic crisis→national crisis→national insecurity→collapse	5. Very high	5. Very high	1. The worst

Table 14. Scenario type.

No.	THE IDENTIFIED RISK (generated by natural disaster)	ESTIMATING THE LIKELIHOOD	ESTIMATING THE GRAVITY	SCENARIO TYPE
1.	Natural risk (earthquake, landslide, volcano, avalanche, tsunami, solar flare, meteor strike, hurricane, drought, frost, etc.)	2. Low	5. Very high	1. The worst

6.3. Threats

A. Estimating the Intention: in this stage, the threats intention will be estimated:

Score level	The intention
1. Very low	Very low intention of threatening
2. Low	Low intention of threatening.
3. Medium	Medium intention of threatening.
4. High	High intention of threatening.
5. Very high	Very high intention of threatening.

B. Estimating the Capability: in this stage, the threats capability will be estimated:

Level	The capability
1. Very low	Very low capability of threatening
2. Low	Low capability of threatening.
3. Medium	Medium capability of threatening.

4. High	High capability of threatening.
5. Very high	Very high capability of threatening.

C. Scenario type: after estimating the intention and capability, the type of scenario will be decided, according with Tables 15 and 16:

- 1. The worst;
- 2. Plausible the worst;
- 3. Moderate.

1. The worst	2. Plausible the worst	3. Moderate

Table 15. Scenario type.

No.	THE IDENTIFIED THREAT (generated by risk)	ESTIMATING THE INTENTION	ESTIMATING THE CAPABILITY	SCENARIO TYPE
1.	Technological threat.	5. Very high	5. Very high	1. The worst
2.	Operative and operational threat	4. High	4. High	2. Plausible the worst
3.	Threat of energetic crisis.	5. Very high	5. Very high	1. The worst
4.	Cyber (terrorist) threat.	5. Very high	5. Very high	1. The worst
5.	Threat of death.	4. High	4. High	3. Moderate
6.	Terrorist threat.	5. Very high	5. Very high	2. Plausible the worst
7.	Threat of energetic crisis.	3. Medium	3. Medium	3. Moderate
8.	Economic threat.	5. Very high	5. Very high	2. Plausible the worst
9.	Threat of energetic crisis.	5. Very high	5. Very high	2. Plausible the worst
10.	Threat of energetic crisis.	4. High	4. High	3. Moderate
11.	Threat of energetic crisis.	4. High	4. High	3. Moderate
12.	Threat of energetic crisis.	3. Medium	3. Medium	3. Moderate
13.	Threat of energetic crisis.	5. Very high	5. Very high	2. Plausible the worst
14.	Financial threat.	4. High	4. High	3. Moderate
15.	Threat of research-development crisis.	4. High	4. High	3. Moderate
16.	Threat of qualified and overqualified staff crisis.	5. Very high	5. Very high	2. Plausible the worst
17.	Threat of sabotage.	5. Very high	5. Very high	2. Plausible the worst
18.	Political and legislative threat.	4. High	4. High	3. Moderate
19.	Threat of energetic crisis.	5. Very high	5. Very high	2. Plausible the worst
20.	Threat of national collapse.	5. Very high	5. Very high	1. The worst
21.	Threat of national collapse.	5. Very high	5. Very high	1. The worst

Table 16. Scenario type.

No.	THE IDENTIFIED THREAT (generated by natural risk)	ESTIMATING THE INTENTION	ESTIMATING THE CAPABILITY	SCENARIO TYPE
1.	Threat of natural disaster (earthquake, landslide, volcano, avalanche, tsunami, solar flare, meteor strike, hurricane, drought, frost, etc.)	5. Very high	5. Very high	1. The worst

6.4. Hazards

A. Estimating the Likelihood: in this stage, the danger likelihood will be estimated:

Score level	The likelihood	Time
1. Very low	It has a very low likelihood of occurring. Normal measures are required to monitor the evolution of the event.	over 20 years
2. Low	The event has a low likelihood of occurring. Efforts are needed to reduce the likelihood and/or mitigate the impact produced.	16 – 20 years
3. Medium	The event has a significant likelihood of occurring. Significant efforts are needed to reduce the likelihood and/or mitigate the impact produced.	11 – 15 years
4. High	The event has a likelihood of occurring. Priority efforts are needed to reduce the likelihood and mitigate the impact produced.	6 – 10 years
5. Very high	The event is considered imminent. Immediate and extreme measures are required to protect the objective, evacuation to a safe location if the impact so requires.	1 – 5 years

B. Estimating the Gravity: in this stage, the danger gravity will be estimated:

Level	Gravity
1. Very low	The event produces a minor disturbance in the activity, without material damage
2. Low	The event causes minor material damage and limited disruption to activity
3. Medium	Injuries to staff, and/or certain losses of equipment, utilities and delays in providing the service.
4. High	Serious staff injuries, significant loss of equipment of installations and facilities, delays and/or interruption of service provision.
5. Very high	The consequences are catastrophic resulting in deaths and serious injuries to staff, major losses in equipment, installations and facilities and termination of service provision.

C. Scenario type: after estimating the likelihood and gravity, the type of scenario will be decided, according with Tables 17 and 18:

- 1. The worst;
- 2. Plausible the worst;
- 3. Moderate.

Table 17. Scenario type.

No.	THE IDENTIFIED HAZARD (generated by threat)	ESTIMATING THE LIKELIHOOD	ESTIMATING THE GRAVITY	SCENARIO TYPE
1.	Hazard of technological instability → black-out.	5. Very high	5. Very high	1. The worst
2.	Hazard of operative and operational insecurity → black-out.	4. High	4. High	2. Plausible the worst
3.	Hazard of national insecurity → lack of national welfare.	5. Very high	5. Very high	1. The worst
4.	Hazard of cyber insecurity → black-out.	5. Very high	5. Very high	1. The worst
5.	Hazard of human insecurity (work accident).	4. High	4. High	3. Moderate
6.	Terrorist Hazard → black-out.	5. Very high	5. Very high	2. Plausible the worst
7.	Hazard of energetic crisis → national insecurity.	3. Medium	3. Medium	3. Moderate
8.	Hazard of energetic crisis → national insecurity.	5. Very high	5. Very high	2. Plausible the worst

9. Hazard of energetic crisis → national insecurity.	5. Very high	5. Very high	2. Plausible the worst
10. Hazard of energetic crisis → national insecurity.	4. High	4. High	3. Moderate
11. Hazard of energetic crisis → national insecurity.	4. High	4. High	3. Moderate
12. Hazard of energetic crisis → national insecurity.	3. Medium	3. Medium	3. Moderate
13. Hazard of energetic crisis → national insecurity.	5. Very high	5. Very high	2. Plausible the worst
14. Hazard of financial crisis → economic insecurity.	4. High	4. High	3. Moderate
15. Hazard of research-development crisis → energetic insecurity	4. High	4. High	3. Moderate
16. Hazard of staff crisis → energetic insecurity.	5. Very high	5. Very high	2. Plausible the worst
17. Hazard of sabotage → energetic insecurity.	5. Very high	5. Very high	2. Plausible the worst
18. Hazard of political and legislative crisis → national insecurity.	4. High	4. High	3. Moderate
19. Hazard of energetic crisis → national insecurity.	5. Very high	5. Very high	2. Plausible the worst
20. Hazard of national collapse → lack of national welfare.	5. Very high	5. Very high	1. The worst
21. Hazard of national collapse → lack of national welfare.	5. Very high	5. Very high	1. The worst

Table 18. Scenario type.

No.	THE IDENTIFIED HAZARD (generated by natural disaster)	ESTIMATING THE LIKELIHOOD	ESTIMATING THE GRAVITY	SCENARIO TYPE
1.	Threat of natural disaster (earthquake, landslide, volcano, avalanche, tsunami, solar flare, meteor strike, hurricane, drought, frost, etc.)	5. Very high	5. Very high	1. The worst

6.5. Agression

A. Estimating the Impact: in this stage, the aggression impact will be estimated:

Level	Impact
1. Very low	The event produces a minor disturbance in the activity, without material damage
2. Low	The event causes minor material damage and limited disruption to activity
3. Medium	Injuries to staff, and/or certain losses of equipment, utilities and delays in providing the service.
4. High	Serious staff injuries, significant loss of equipment of installations and facilities, delays and/or interruption of service provision.
5. Very high	The consequences are catastrophic resulting in deaths and serious injuries to staff, major losses in equipment, installations and facilities and termination of service provision.

B. Scenario type: after estimating the aggression impact, the type of scenario will be decided, according with Tables 19 and 20:

- 1. The worst;
- 2. Plausible the worst;
- 3. Moderate.

1. The worst	2. Plausible the worst	3. Moderate

Table 19. Scenario type.

No.	THE IDENTIFIED AGRESSION (generated by danger)	ESTIMATING THE IMPACT	SCENARIO TYPE
1.	Cyber attack → black-out.	5. Very high	1. The worst
2.	Physical attack.	4. High	3. Moderate
3.	Terrorist attack: armed/ bomb → black-out.	5. Very high	2. Plausible the worst
4.	Attack from the inside (theft/armed attack/cyber attack) → black-out	5. Very high	2. Plausible the worst

Table 20. Scenario type.

No.	THE IDENTIFIED AGRESSION (generated by natural disaster)	ESTIMATING THE IMPACT	SCENARIO TYPE
1.	Attacks caused by natural disasters.	5. Very high	1. The worst

6.6. Prioritizing Scenarios

A. The identification of the worst scenarios: according with Table 21. [1–4]

Table 21. The identification of the worst scenarios.

No.	IDENTIFICATION OF THE SCENARIO	SCENARIO TYPE	THE GENERATING ELEMENT
1	Poor management of the transmission operator activity (exploitation, maintenance and development) of The Power Transmission Grid installations.	THE WORST	Vulnerability
2	Instability and insecurity of The National Power System caused by lack or precarious investments in the power infrastructure.		Vulnerability
3	The precariousness of Cyber Security activity.		Vulnerability
4	Lack of electricity – possible local, area, regional or national black-out.		Vulnerability
5	The dependence of national systems on electricity.		Vulnerability
6	Risk of technical incident (isolated/associated), technical disturbance or damage.		Risk
7	Risk of partial or total disconnection of The National Power System – black-out.		Risk
8	Risk of cyber attack.		Risk
9	Risk of energetic crisis		Risk
10	Risk of energetic crisis→national crisis→national insecurity→collapse		Risk
11	Natural risk (earthquake, landslide, volcano, avalanche, tsunami, solar flare, meteor strike, hurricane, drought, frost, etc.)		Risk
12	Technological threat.		Threat
13	Threat of energetic crisis.		Threat
14	Cyber (terrorist) threat.		Threat
15	Threat of national collapse.		Threat
16	Threat of national collapse.		Threat
17	Threat of natural risk (earthquake, landslide, volcano, avalanche, tsunami, solar flare, meteor strike, hurricane, drought, frost, etc.)		Threat
18	Hazard of technological instability (incident / damage) → black-out.		Hazard
19	Hazard of national insecurity → lack of national welfare.		Hazard
20	Hazard of cyber insecurity → black-out.		Hazard
21	Hazard of national collapse → lack of national welfare.		Hazard
22	Hazard of national collapse → lack of national welfare.		Hazard

23	Hazard of natural risk (earthquake, landslide, volcano, avalanche, tsunami, solar flare, meteor strike, hurricane, drought, frost, etc.)		Hazard
24	Cyber attack → black-out.		Agression
25	Attacks caused by natural disasters.		Agression

B. Choosing the worst scenarios for the assessment: according with Table 22. [1–4]

Table 22. Choosing the worst scenarios for assessment.

No.	IDENTIFICATION OF THE SCENARIO FOR THE ASSESSMENT
1	Poor management of the transmission operator activity (exploitation, maintenance and development) of the Power Transmission Grid installations → Risk of technical incident (isolated/associated), technical disturbance or damage → Technological threat → Hazard of technological instability (incident / damage) → black-out.
2	Risk of natural disaster → Threat of natural disaster → Hazard of natural disaster → Attacks caused by natural disasters (earthquake, landslide, volcano, avalanche, tsunami, solar flare, meteor strike, hurricane, drought, frost, etc.).

7. Conclusions

Following the analysis of the instability and insecurity elements within the National Power System, the following were identified: 7 dysfunctions, 11 deficiencies, 3 non-compliances, 21 vulnerabilities, 21 risks, 1 risk from outside, 21 threats, 1 threat from outside, 21 hazards, 1 hazard from outside, 4 aggressions and 1 aggression from outside.

Following the prioritization of the identified instability and insecurity elements within the National Power System (7 dysfunctions, 11 deficiencies, 3 non-compliances, 21 vulnerabilities, 21 risks, 21 threats, 1 threat from outside, 21 hazards, 1 hazards from outside, 4 aggressions and 1 aggression from outside), the following types of risk scenarios have been highlighted:

- Vulnerabilities: 5 the worst scenarios; 8 the plausible the worst; 8 moderate scenarios;
- Risks: 6 the worst scenarios; 8 the plausible the worst; 8 moderate scenarios;
- Threats: 6 the worst scenarios; 8 the plausible the worst; 8 moderate scenarios;
- Dangers: 6 the worst scenarios; 8 the plausible the worst; 8 moderate scenarios;
- Aggression: 2 the worst scenarios; 2 the plausible the worst; 1 moderate scenarios.

In total is 25 the worst scenarios, 34 plausible the worst and 33 moderate scenarios.

Following the highlighting of the 25 the worst scenarios, the authors propose that only 2 risk scenarios with very high probability and severity, may endanger the malfunctioning of the National Power System (black-out), to be evaluated in future paper:

- Poor management of the transmission operator activity (exploitation, maintenance and development) of the Power Transmission Grid installations → Risk of technical incident (isolated/associated), technical disturbance or damage → Technological threat → Hazard of technological instability (incident / damage) → black-out;
- Risk of natural disaster → Threat of natural disaster → Hazard of natural disaster → Attacks caused by natural disasters (earthquake, landslide, volcano, avalanche, tsunami, solar flare, meteor strike, hurricane, drought, frost, etc.).

References

1. Nicolae Daniel Fiță, Mila Ilieva Obretenova, Florin G. Popescu, Romanian Power System – European energy security generator, LAP – Lambert Academic Publishing, ISBN: 978-620-7-46269-8, 2024.

2. Nicolae Daniel Fiță, Dan Codrut Petrilean, Ioan Lucian Diodiu, Andrei Cristian Rada, Adrian Mihai Schiopu, Florin Muresan-Grecu, Analysis of the causes of power crises and their impacts on energy security, Proceedings of International Conference on Electrical, Computer and Energy Technologies –

- ICECET 2204, July 2024, Sydney, Australia, Publisher IEEE, Date added to IEEE Explore: 08 October 2024, www.icecet.com, DOI: 10.1109/ICECET61485.2024.10698524.
3. Nicolae Daniel Fiță, Adina Tătar, Mila Ilieva Obretenova, Security risk assessment of critical energy infrastructures, LAP – Lambert Academic Publishing, ISBN: 978-620-7-45824-0, 2024.
 4. Nicolae Daniel Fiță, Mila Ilieva Obretenova, Adrian Mihai Șchiopu, National Security – Elements regarding the optimisation of Energy Sector, LAP – Lambert Academic Publishing, ISBN: 978-620-7-45693-2, 2024.
 5. ISO 31000:2018 - Risk management – Guidelines.
 6. Kezunovic, M.; Dobson, I.; Dong, Y. Impact of extreme weather on power system blackouts and forced outages: New challenges. In Proceedings of the 7th Balkan Power Conference, Šibenik, Croatia, 10–12 September 2008; pp. 1–5.
 7. Panteli, M.; Mancarella, P. Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies. *Electr. Power Syst. Res.* 2015, 127, 259–270.
 8. Li, T.; Luo, B.; Liu, L.; Wu, T. Wind accident analysis of transmission line in China Southern Power Grid's Coastal Regions. In Proceedings of the 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT), Changsha, China, 26–29 November 2015; pp. 1700–1704.
 9. Panteli, M.; Mancarella, P. Modeling and Evaluating the Resilience of Critical Electrical Power Infrastructure to Extreme Weather Events. *IEEE Syst. J.* 2015, 11, 1733–1742.
 10. Cadini, F.; Agliardi, G.L.; Zio, E. A modeling and simulation framework for the reliability/availability assessment of a power transmission grid subject to cascading failures under extreme weather conditions. *Appl. Energy* 2017, 185, 267–279.
 11. Liu, Y. Short-term operational reliability evaluation for power systems under extreme weather conditions. In Proceedings of the 2015 IEEE Eindhoven PowerTech, Eindhoven, The Netherlands, 29 June–2 July 2015; pp. 1–5.
 12. Anvari, M.; Lohmann, G.M.; Wächter, M.; Milan, P.; Lorenz, E.; Heinemann, D.; Tabar, M.R.R.; Peinke, J. Short term fluctuations of wind and solar power systems. *New J. Phys.* 2016, 18, 063027.
 13. Pahwa, S.; Scoglio, C.M.; Scala, A. Abruptness of Cascade Failures in Power Grids. *Sci. Rep.* 2014, 4, 3694.
 14. Gan, Y.; Hu, Y.; Ruan, J.; Du, Z.; Liu, C.; Du, W. Analysis and Prevention of Main Natural Disasters of 500kV Transmission Lines in Central China Power Grid. *Electr. Power Constr.* 2012, 6, 37–42.
 15. Kiel, E.S.; Kjølle, G.H. The impact of protection system failures and weather exposure on power system reliability. In Proceedings of the International Conference on Environment and Electrical Engineering and 2019 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Genova, Italy, 10–14 June 2019; pp. 1–6.
 16. Jufri, F.H.; Widiputra, V.; Jung, J. State-of-the-art review on power grid resilience to extreme weather events: Definitions, frameworks, quantitative assessment methodologies, and enhancement strategies. *Appl. Energy* 2019, 239, 1049–1065.
 17. Matko, M.; Golobič, M.; Kontić, B. Reducing risks to electric power infrastructure due to extreme weather events by means of spatial planning: Case studies from Slovenia. *Utilities Policy* 2017, 44, 12–24.
 18. Chen, X.; Sun, K.; Cao, Y.; Wang, S. Identification of Vulnerable Lines in Power Grid Based on Complex Network Theory. In Proceedings of the 2007 IEEE Power Engineering Society General Meeting, Tampa, FL, USA, 23 July 2007; pp. 1–6.
 19. Arianos, S.; Bompard, E.; Carbone, A.; Xue, F. Power grid vulnerability: A complex network approach. *Chaos: Interdiscip. J. Nonlinear Sci.* 2009, 19, 013119.
 20. Pagani, G.A.; Aiello, M. The Power Grid as a complex network: A survey. *Phys. A Stat. Mech. Its Appl.* 2013, 392, 2688–2700.
 21. Cuadra, L.; Salcedo-Sanz, S.; Del Ser, J.; Jiménez-Fernández, S.; Geem, Z.W.; Cuadra, L.; Salcedo-Sanz, S.; Del Ser, J.; Jiménez-Fernández, S.; Geem, Z.W. A Critical Review of Robustness in Power Grids Using Complex Networks Concepts. *Energies* 2015, 8, 9211–9265.
 22. Li, Q.; Li, H.Q.; Huang, Z.M.; Li, Y.Q. Power system vulnerability assessment based on transient energy hybrid method. *Power Syst. Protect. Control.* 2013, 41, 1–6.
 23. Li, X.; Qi, Z. Impact of cascading failure based on line vulnerability index on power grids. *Energy Syst.* 2021, 1–26.

24. Abedi, A.; Gaudard, L.; Romero, F. Review of major approaches to analyze vulnerability in power system. *Reliab. Eng. Syst. Saf.* 2019, 183, 153–172.
25. Johansson, J.; Hassel, H.; Zio, E. Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. *Reliab. Eng. Syst. Saf.* 2013, 120, 27–38.
26. Ouyang, M. Comparisons of purely topological model, betweenness based model and direct current power flow model to analyze power grid vulnerability. *Chaos Interdiscip. J. Nonlinear Sci.* 2013, 23, 023114.
27. Wei, X.; Gao, S.; Huang, T.; Bompard, E.; Pi, R.; Wang, T. Complex Network-Based Cascading Faults Graph for the Analysis of Transmission Network Vulnerability. *IEEE Trans. Ind. Inform.* 2018, 15, 1265–1276.
28. Wang, W.; Song, Y.; Li, Y.; Jia, Y. Research on Cascading Failures Model of Power Grid Based on Complex Network. In *Proceedings of the 2020 Chinese Control and Decision Conference (CCDC)*, Hefei, China, 22–24 August 2020; pp. 1367–1372.
29. Alin E. Cruceru, Florin G. Popescu, Daniel N. Fita, Marius D. Marcu, Razvan C. Olteanu, Adrian M. Schiopu, Gabriela Popescu, *Current Approaches in Engineering Research and Technology*, Vol. 10, Chapter 4: Exploring the Dimensions of Energy Security in Relation to the National Power Grid, Book Publisher International, India ISBN 978-81-983173-4-6 (Print), ISBN 978-81-983173-0-8 (eBook), DOI: 10.9734/bpi/caert/v10/3282.
30. Moraru, R.I., Păun, A.P., Dura, C.C., Dinulescu, R., Potcovaru, A-M. Analysis of the drivers of Occupational Health and Safety performance disclosures by Romanian companies, *Economic Computation and Economic Cybernetics Studies and Research*, Issue 3, 2020, pp. 197 – 214, <https://doi.org/10.24818/18423264/54.3.20.12>.
31. Darabont, D.C., Moraru, R.I., Antonov, A.E., Bejinariu, C. (2017), Managing new and emerging risks in the context of ISO 45001 standard, *Quality - Access to Success*, Volume 18, Supplement 1, pp. 11-14.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.