sustainability

Article

Sustainability Management Through the Assessment of Instability and Insecurity Risk Scenarios in Romania's Energy Critical Infrastructures

Dan Codruț Petrilean [1], Nicolae Daniel Fîță [1], Gabriel Dragoș Vasilescu [2], Mila Ilieva-Obretenova [3], Dorin Tataru [1], Emanuel Alin Cruceru [4], Ciprian Ionuț Mateiu [1,*], Aurelian Nicola [1], Doru-Costin Darabont [5], Alin-Marian Cazac [6,*] and Costica Bejinariu [6,7]

[1] Faculty of Mechanical and Electrical Engineering, University of Petrosani, 20 University Street, 332006 Petrosani, Romania; danpetrilean@upet.ro (D.C.P.); daniel.fita@yahoo.com (N.D.F.); dorintataru@upet.ro (D.T.); aureliannicola@upet.ro (A.N.)

[2] National Institute for Research and Development in Mine Safety and Protection to Explosion—INSEMEX, 332047 Petrosani, Romania; dragos.vasilescu@insemex.ro

[3] Mining Electromechanics, Automation of Production Systems Department, University of Mining and Geology, St. Ivan Rilski Sofia, 1700 Sofia, Bulgaria; mila.ilieva@mgu.bg

[4] Industrial Engineering Doctoral School, National University of Science and Technology POLITEHNICA Bucharest, Splaiul Independentei No. 313, Sector 6, 060042 Bucharest, Romania; alincruceru1988@gmail.com

[5] National Research and Development Institute on Occupational Safety—I.N.C.D.P.M. "Alexandru Darabont", 35A Ghencea Blvd., Sector 6, 061692 Bucharest, Romania; darabont_d@yahoo.com

[6] Faculty of Materials Science and Engineering, Gheorghe Asachi Technical University of Iasi, 67 Dimitrie Mangeron Str., 700050 Iasi, Romania; costica.bejinariu@academic.tuiasi.ro

[7] Academy of Romanian Scientists, Ilfov 3, 050044 Bucharest, Romania

* Correspondence: cipri_mci@yahoo.com (C.I.M.); alin-marian.cazac@academic.tuiasi.ro (A.-M.C.); Tel.: +40-722-531-852 (C.I.M.); +40-741-940-768 (A.-M.C.)

Abstract: In the current context of sustainability management and energy insecurity, amplified by the military instability determined by the war between Russia and Ukraine, and the increasingly frequent occurrence of a series of plausible scenarios for disasters or energy blackouts worldwide, this work is a real and applicable model for regional states that would like to critically analyze the situation of their energy security through identifying all the plausible risk scenarios targeting the energy critical infrastructures. The study has identified and assessed two of the most plausible risk scenarios (a natural disaster and a terrorist attack) in the case of a strategic power substation of 220 kV, 400 kV, or 750 kV undergoing a blackout effect. After having assessed the risks, the safety strategy for Romania's national power system has been elaborated together with the safety strategy for the European Power system-ENTSO-E (European Network of Transmission System Operators for Electricity). The results of the study match other specialized works from different European countries and might represent a model for other types of energy safety risk assessments and for other types of critical infrastructures that are vital for the modern European society and for sustainability management.

Keywords: sustainability management; risk scenarios; energy critical infrastructure; energy safety; Romania's national energy system

Academic Editor: Jarosław Górecki

Received: 30 January 2025
Revised: 10 March 2025
Accepted: 12 March 2025
Published: 26 March 2025

Citation: Petrilean, D.C.; Fîță, N.D.; Vasilescu, G.D.; Ilieva-Obretenova, M.; Tataru, D.; Cruceru, E.A.; Mateiu, C.I.; Nicola, A.; Darabont, D.-C.; Cazac, A.-M.; et al. Sustainability Management Through the Assessment of Instability and Insecurity Risk Scenarios in Romania's Energy Critical Infrastructures. *Sustainability* **2025**, *17*, 2932. https://doi.org/10.3390/su17072932

1. Introduction—The Condition of the Romanian National Energy System

In the context of increasing competition for power and influence in the domain of energy and, implicitly, in the economic area, at a regional and global level, electric energy plays the most important part in a state's position and its role within the international relations system by providing energy security. The lack of pertinent analyses of cross-border critical energy infrastructures (power plants, power substations, and powerlines) of states that are less developed from the point of view of energy and the economy has determined the increase in speculation, as well as a series of "energy monopoles" that concern the control of the main powerlines, markets, and electric energy prices. Under such circumstances, energy security is not only an external policy objective, but has become an important and constant preoccupation for the international energy community with a view to providing European and global security. In order to prevent a collapse of the national energy system, each European state has energy strategies for protecting and securing their critical energy infrastructures that facilitate their population's access to electric energy, which represents an important factor for national and European security. These energy security strategies only develop when preventively assessing the degree of vulnerability of the energy critical infrastructures, through identifying all possible risk security scenarios determining instability and energy insecurity effects. It is well known that an energy system includes all critical infrastructures (power plants, power substations, and overhead or underground powerlines), exploited and administered in accordance with a unitary conception, which contributes to the production, transportation, and distribution of electric energy to the consumers; the approach and critical analysis of the Romanian energy system (Figure 1) is a matter of national security as the lack of electricity could determine damages to the Romanian industry and economy that are entirely dependent on electric energy (see Figure 2) [1].

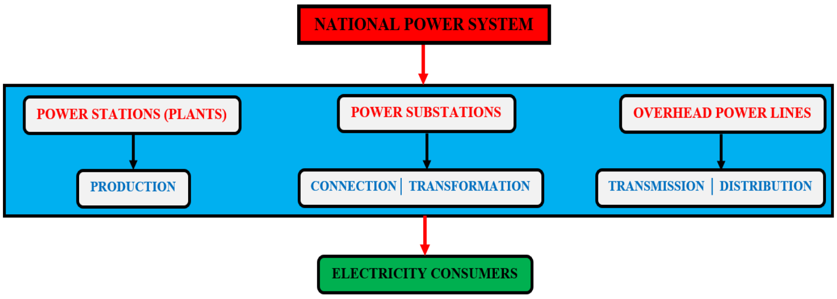

Figure 1. Critical infrastructure of the Romanian power system.

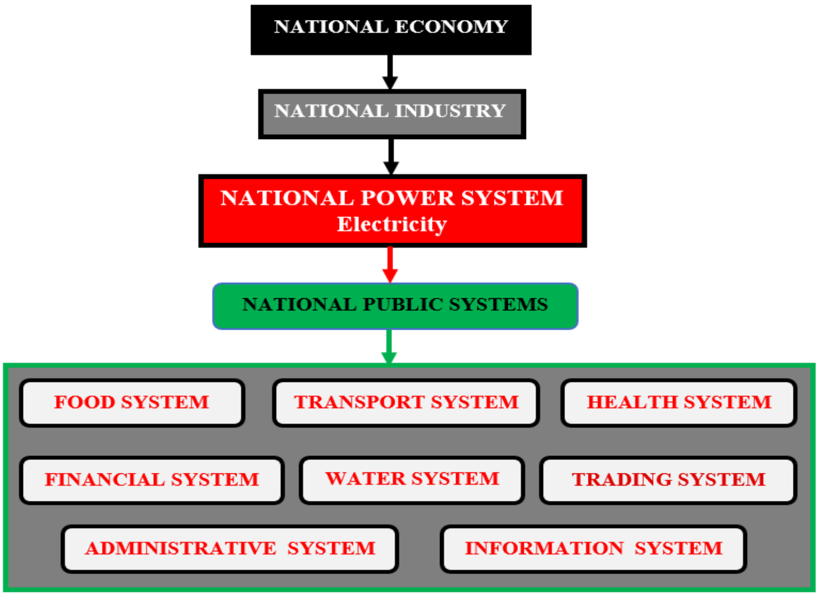

Figure 2. Dependence of the national industry and economy on electric energy.

Table 1 and Figure 3 display the European connections of the Romanian power system. [2].

Table 1. European connections of the national power system with ENTSO-E.

Country	Type of Connection (Overhead Electric Line)	Voltage Level
UKRAINE	Roșiori—Mukacevo Isaccea—South Ukraine	400 kV—connection to EU, through ENTSO-E 400 kV (750 kV)—disabled line
HUNGARY	Nădab—Bekescsaba Arad—Sandorfalva	400 kV—connections to EU, through ENTSO-E
SERBIA	Reșița—Pancevo 2 Porțile de Fier—Djerdap	400 kV—connections to EU
BULGARIA	Țânțăreni—Kosloduy Rahman—Dobrudja Stupina—Varna	400 kV—connections to EU, through ENTSO-E 400 kV (750 kV)—connection to EU
REPUBLIC OF MOLDOVA	Isaccea—Vulcănești	400 kV

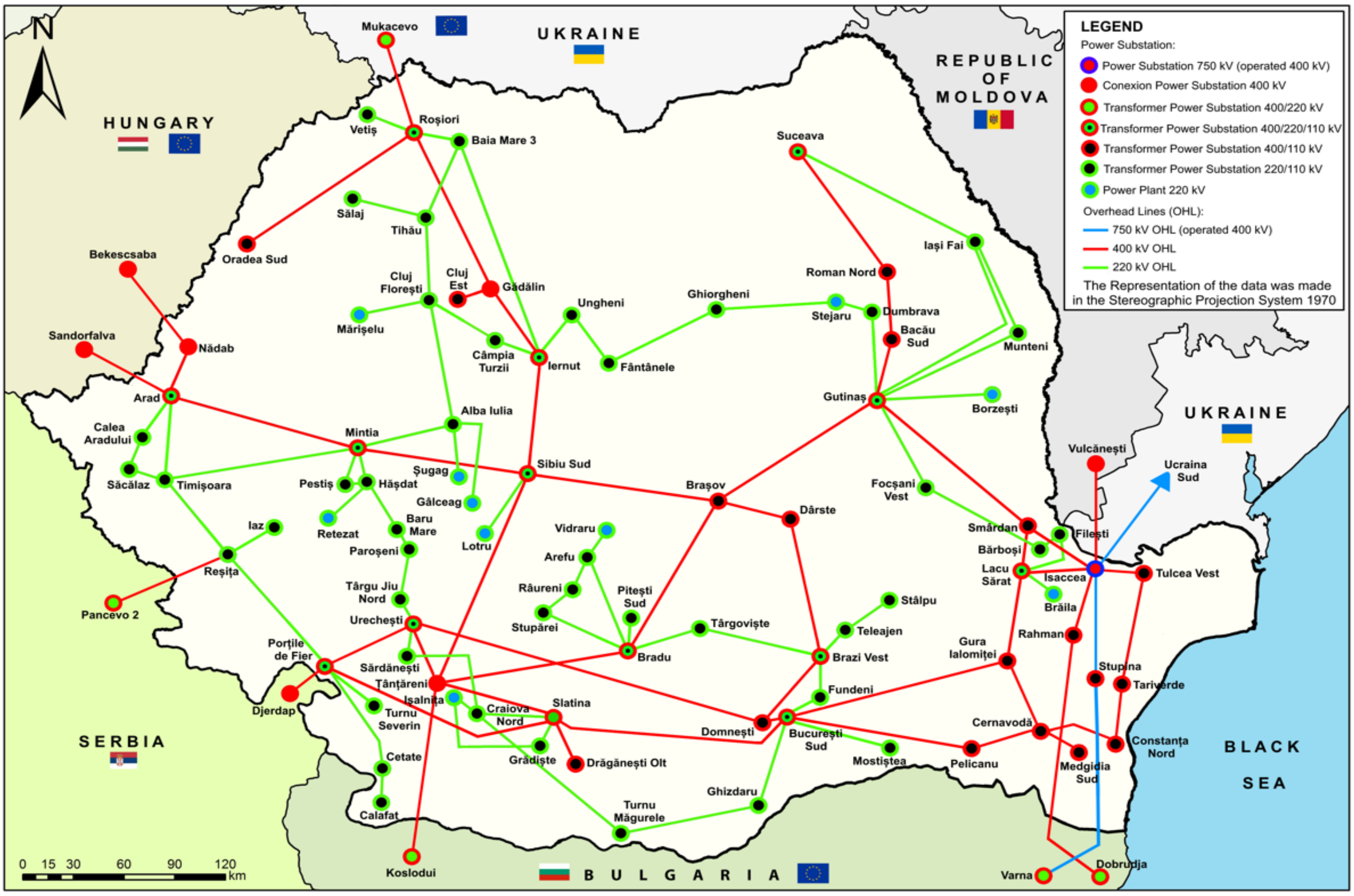

Figure 3. Romania's power system.

1.1. Previous Studies

Electricity crises have been a topic of interest to many researchers and authors, with economic, political, and environmental implications. Below are some authors and studies that have addressed energy crises, especially electricity crises, from different perspectives.

(a) Global and economic energy crises: Studies on electricity crises are often linked to general energy crises, which include energy resource shortages and fluctuating fossil fuel prices. A relevant example can be found in the analysis of the global energy economy, as discussed in Thomas Homer-Dixon's work on energy security and the conflict generated by scarce resources. In his book, *The Upside of Down: Catastrophe, Creativity, and the Renewal of Civilization* (2006), Homer-Dixon examines how resource crises can trigger political and economic instability, and electricity plays a key role in this dynamic [3].

(b) Economic theories of energy crises: An influential study in the analysis of electricity crises was conducted by James O'Connor in *The Fiscal Crisis of the State* (1973), which argues that energy crises are often linked to economic structure and state policies. He suggests that too much dependence on external energy sources can undermine the stability of national economies, and fluctuations in energy prices can generate economic instability [4].

(c) Technical aspects of electricity crises: Another area of research is related to electricity generation and distribution technologies, which can contribute to energy crises. Paul Sabin in his work *The Bet: Paul Ehrlich, Julian Simon, and Our Gamble over Earth's Future* iscusses how technological innovations can play an important role in preventing or worsening electricity crises through advances in renewable energy sources, energy storage, and energy efficiency [5].

(d) Impact of energy policies and climate change: Electricity crises can be aggravated by unsustainable energy policies or the effects of climate change, which can reduce the availability of traditional energy sources. For example, in his study *Energy Crisis: A Global Problem* (2011), Richard Heinberg points out how the transition from fossil energy sources to renewable sources can help prevent long-term energy crises, but also how the urgent need to combat climate change can create new challenges in ensuring stable electricity production [6].

(e) Energy crisis management: In addressing electricity crises, authors such as Pablo del Rio Gonzalez (2009) explored crisis management in the context of national and regional energy systems, highlighting how effective policies and the interconnection of electricity grids can improve the impact of electricity crises [7].

Relevant authors and contributions:

(a) Jean-Michel Glachant (2017) has studied the impact of energy crises on electricity markets and how market regulation and alignment of regional strategies can play a key role in managing electricity crises [8].

(b) David MacKay, in *Sustainable Energy—Without the Hot Air* (2009), discusses how energy crises can be avoided through sustainable strategies, based on renewable energy sources and innovative energy storage solutions [9].

In conclusion, studies on electricity crises are multidisciplinary, addressing economic, political, technical, and environmental issues. From the impact of energy policies and global interdependence to technological innovations and resource management, researchers are aware of the complexity of this phenomenon.

1.2. Recent Evolutions

The study and the need to approach the power systems is required by the new elements of instability and insecurity in our modern and vulnerable society, which are unpredictable, subtle, and sometimes perverted, and might determine extreme damage to all states, irrespective of their geopolitical or geo-economic condition. All modern world states own energy security strategies, which, most of the time, include sensitive, confidential and even secret data. The security risk assessments of the energy critical infrastructures are quite important as they identify almost all the elements of instability and insecurity (vulnerabilities, threats, risks, and dangers). Based on them, measures for eliminating or stopping such instability and insecurity elements might be conceived, and strategies for the security and protection of the energy critical infrastructures and energy security strategies might be developed.

Within the new world order that makes up the security environment, all modern states own a centralized or, sometimes, isolated energy system (in the case of island states), which provide electric energy to households and industrial consumers; for this reason, the authors consider that it is vital to approach this system from the point of view of security, which includes the manner of identifying and assessing all the plausible risk scenarios regarding the instability of critical infrastructures belonging to the power systems [10–14].

Worldwide, the setting forth, studies, and research around energy critical infrastructures are of great interest and topical as they represent the most vulnerable point of a society. The vulnerabilities, dangers, and threats to critical infrastructures become interest domains not only for military and intelligence specialists but also for civilian specialists that operate or own such infrastructures [15–17].

American specialists in the United States Department of Energy have elaborated a methodology that is able to assess the vulnerability of a power system together with the risks, threats, and dangers determined by it, which could result in blackouts [18].

Researchers, Hasan Haes Alhelou, Mohamad Esmail Hamedani-Golshan, and Takawira Cuthbert Njenda, at Isfahan University of Technology in Iran, have devised a pertinent and specific analysis that regards the causes and errors determining blackouts in various energy systems on three continents: America, Asia, and Europe [19].

In Romania, studies and research regarding energy critical infrastructures are of great interest and topicality as this is a vast, multidisciplinary, cross-disciplinary, and interdisciplinary domain, without which energy security and national welfare would be endangered [20,21].

Specific elements of energy insecurity being examined are security supply with electricity and risks caused by natural calamities and terrorist attacks, but there are also other possible risks like cyberattacks or industrial failures (unsafe power systems) to consider.

The risk assessment methodology used in this paper is derived from the Risk Management ISO 31000:2018 and is composed of the approximation of probability, impact, and risk matrix across five levels (very low, low, average, high, and very high) [22].

As a result of our critical analysis of Romania's national power system carried out in this work, the following outcomes are highlighted [23,24]:

1. Identifying the two most plausible serious risk scenarios:
   a. Risk scenario 1—220–750 kV Power Substation Natural Calamity → Blackout;
   b. Risk scenario 2—220–750 kV Power Substation Terrorist Attack → Blackout.
2. Assessment of risk scenarios by means of the following:
   a. Probability approximation;
   b. Seriousness or impact level approximation;
   c. Risk level calculation;
   d. Recalculation of risk level following the proposed measures.
3. Elaboration of the security strategy for Romania's national power system following the proposed measures, which can improve and strengthen the European Power System ENTSO-E.

If each individual state within the ENTSO-E assesses its vulnerabilities and risks in the case of a natural disaster or terrorist attack and devises protection measures, the European Power System ENTSO-E will becomes secure, adaptable, and resilient.

The results and usefulness of this study match those of other specialized works in European states and could represent a model for other types of energy security risk assessments for all kinds of critical infrastructures vital for the European modern society.

The European study, developed by the European Network of Transmission System Operators for Electricity—ENTSO-E, with the title ENTSO-E Strategic Roadmap (published in February 2024, in Chapter 2, Building Blocks of the Strategy (pillar 1: A Power System for a Carbon-Neutral Europe and pillar 2: A Secure and Efficient Power System for Europe), discusses the same issues regarding the safety and security of the European Power System, which is in line with the work and conclusions in this paper.

The novel and original elements set forth in this work are the following:

1. Identification and technical description through the analysis and manner of approach towards the critical infrastructures connected to Europe, and the elements providing connection and interdependence with other critical infrastructures belonging to Romania's national power system;
2. Identification, through critical analysis, of the most serious plausible risk scenarios;
3. Description, through cause–effect critical analysis, of all most serious plausible risk scenarios;
4. Sequence scrolling through developing all the stages of the risk scenarios identified, from source to effect;
5. Assessment of risk scenarios within Romania's national power system;
6. Elaboration of the security strategy for Romania's national power system;
7. Adaptation and flexible use of the study for all energy systems that include critical infrastructures.

This paper comes to the aid of the Romanian electricity transmission operator, Transelectrica, which of course has an intervention and preventive plan in the case of an energy crisis. In such a case, Romania has overhead powerlines (according to Table 1) of interconnection with neighboring countries that offer high reliability to the Romanian power system.

2. Critical Analysis and Results Regarding the Most Plausible Serious Risk Scenarios

During this stage, the following essential actions are required: identifying risk scenarios, describing risk scenarios, sequence scrolling of the risk scenarios, and assessing risk scenarios.

2.1. Identifying Risk Scenarios

The two most plausible serious risk scenarios have been identified after a critical analysis of Romania's national power system [25–27]:

1. Risk scenario 1—220–750 kV Power substation natural calamity → Blackout;
2. Risk scenario 2—220–750 kV Power substation terrorist attack → Blackout.

2.2. Describing the Risk Scenarios

The two risk scenarios (causes and effects) are described below.

1. Risk scenario 1—220–750 kV Power substation natural calamity → Blackout.

The causes and effects of risk scenario 1 are described in Table 2.

Table 2. Causes and effects of risk scenario 1.

Causes:	Effects:
1. Earthquakes; 2. Floods; 3. Tsunamis; 4. Avalanches; 5. Fires; 6. Meteorite showers; 7. Poor/wrong seismic designing of the electric stations; 8. Operative/dispatch personnel who are not specialized for dealing with crises; 9. Lack of work procedures in the stations during crises; 10. Lack of/non-compliance/ignorance of national/European procedures in case of natural calamity; 11. Lack of training in the field of risk management.	1. Possible deaths; 2. Possible accidents with serious effects; 3. Fires; 4. Huge material damages determined by the lack of electric energy; 5. Huge material damages determined by the interdependence among other systems; 6. Possibility of a local, regional, or national blackout; 7. Energy—economic collapse; 8. Possible crises; 9. Energy insecurity; 10. Economic insecurity; 11. National insecurity.

2. ***Risk scenario 2—220–750 kV Power substation terrorist attack → Blackout.***

The causes and effects of risk scenario 2 are described in Table 3.

Table 3. Causes and effects of risk scenario 2.

Causes:	Effects:
1. Explosions after a terrorist attack followed by fires; 2. Ignorance of fire security standards; 3. Lack of training/poor training of personnel in the management of critical protection infrastructures; 4. Lack of specialized personnel in the domain of fire extinguishing; 5. Lack of physical security personnel; 6. Cybernetic attacks; 7. Insecurity of hardware systems; 8. Insecurity of software systems; 9. Insecurity of secret data transmission systems of critical infrastructures; 10. Lack of personnel specialized in cybernetic security; 11. Insecurity of SCADA (Supervisory Control and Data Acquisition) systems; 12. Operating with insecure and/or nonperforming programs; 13. Lack of secure communication with the National Energy Dispatch, the Territory Energy Dispatch and those in charge of cybernetic security; 14. Lack of cybernetic investments.	1. Possible deaths; 2. Possible accidents followed by serious effects; 3. Fires; 4. Access to secret information about the Romanian national power system by unauthorized individuals; 5. Use of secret information about Romania's national power system for the purpose of terrorism; 6. Sudden shutdown of remote-controlled energy equipment by hackers; 7. Huge material damages determined by the lack of electric energy; 8. Huge material damages determined by the interdependence with other systems; 9. Possibility of a local, regional, or national blackout; 10. Energy—economic collapse; 11. Possible crises; 12. Energy insecurity; 13. Economic insecurity; 14. National insecurity.

2.3. Sequence Scrolling of Risk Scenarios

The sequence scrolling of risk scenario 1 is described below

RISK SCENARIO 1
220–750 kV POWER SUBSTATION NATURAL CALAMITY
Extreme meteorological phenomena (earthquakes, floods, avalanches, volcanoes, fires, tsunamis, meteorite showers, etc.) on → Energy critical infrastructures (energy groups in power substations, overhead powerlines for transporting electric energy 220–750 kV, power substations 220–750 kV) → Instability of the national power system → Blackout

The sequence scrolling of risk scenario 2 is described below

RISK SCENARIO 2
220 kV–750 kV POWER SUBSTATION TERRORIST ATTACK
Explosion determined by a bomb (terrorist) and/or a cybernetic attack determined by a virus (hacker) → Physical and/or cybernetic security personnel errors on → Energy critical infrastructures (energy groups in power substations, overhead powerlines for transporting electric energy 220 kV–750 kV, 220 kV–750 kV power substations) → Instability of the national power system → Total exit from operation of the national power system → Blackout

2.4. Assessment of the Risk Scenarios

The two risk scenarios are further assessed:

1. Risk scenario 1—Natural calamity → Total/partial operation exit of the national power system;
2. Risk scenario 2—Terrorist attack → Total/partial operation exit of the national power system.

A. Risk scenario 1—Natural calamity → Total/partial shutting of the national power system;

(a) Settling the probability

With a view to settling occurrence probability, the following probability scale has been adopted:

Associated Level/Score		**Defining Probability**	**Periods**
X	**1.** **Very low**	The event has a very low occurrence probability. Usual measures for monitoring the evolution of the event are required.	Over 13 years
	2. **Low**	The event has a low occurrence probability. Efforts are required to reduce the probability and/or reduce the impact produced.	10–12 years
	3. **Average**	The event has a significant occurrence probability. Significant efforts are required to reduce the probability and/or reduce the impact produced.	7–9 years
	4. **High**	The event is probable to occur. Priority efforts are required to reduce the probability and attenuate the impact produced.	4–6 years
	5. **Very high**	The event is considered imminent. Immediate and extreme measures are required for protecting the objective and for evacuation to a safe location in the case that the impact requires this.	1–3 years

The colors green, brown, yellow, orange and red represent probability level (green is very low, brown is low, yeloow is average, orange is high and red is very high)

(b) Settling the seriousness of the consequences of the proposed scenario

The analysis of vulnerabilities and capabilities is displayed in Table 4.

Table 4. Analysis of vulnerabilities and capabilities for risk scenario 1.

Scenario 1: Failure **Vulnerabilities and Capabilities**	**Level**
1. Poor/wrong design of the power substations and overhead powerlines against earthquakes	Very low
	Low
	Average
	High
	[✓ Very high]
2. Risk of tsunami occurrence after an earthquake	[✓ Very low]
	Low
	Average
	High
	Very high
3. Lack of personnel or insufficiently trained personnel for crisis, natural calamity, or risk management.	Very low
	Low
	Average
	High
	[✓ Very high]

Vulnerability 1 and 3 is very high and vulnerability 2 is very low.

2.4.1. Impact

We are going to choose the highest of the seriousness impact levels, in accordance with Table 5.

Table 5. Analysis of the impact for risk scenario 1.

Impacts	**Level**	
1. Huge damages determined by the lack of electric energy	1. Very low	Temporarily
	2. Low	Important damages
	3. Average	Average damages
	4. High	High damages
	[✓ 5. Very high]	[✓ Very high damages]
2. Huge damages determined by the interdependence with other systems	1. Very low	0–10% of VIC
	2. Low	11–20% of VIC
	3. Average	21–30% of VIC
	4. High	31–40% of VIC
	[✓ 5. Very high]	[✓ Over 41% of VIC]
3. Potential damages of the environment	1. Very low	0–20%
	2. Low	21–40%
	3. Average	41–60%
	4. High	61–80%
	[✓ 5. Very high]	[✓ Over 81%]
4. Powerful social impacts	1. Very low	0–10% of PC
	2. Low	11–20% of PC
	3. Average	21–30% of PC
	4. High	31–40% of PC
	[✓ 5. Very high]	[✓ Over 41% of PC]

VIC—Volume of invested capital; PC—Public confidence.

Associated Level/Score		Seriousness of Consequences
	1. Very low	The event determines a minor disruption of the activity, without material damages.
	2. Low	The event determines minor material damages and limited disruption of the activity.
	3. Average	Injuries of the personnel and/or certain equipment and utilities losses as well as delays in providing the service.
	4. High	Serious injuries of the personnel, significant equipment, installation, and facility losses, and delays and/or shutting of services.
X	**5. Very high**	Consequences are catastrophic, resulting in deaths and serious injuries of the personnel, important equipment, installations, and facility losses, and shutting of the service.

The colors green, brown, yellow, orange and red represent seriousness of consequences level (green is very low, brown is low, yeloow is average, orange is high and red is very high)

(c) Calculation of the risk level

PROBABILITY					
Very high 5	🟫	🟨	🟧	🟥	🟥
High 4	🟫	🟨	🟨	🟧	🟥
Average 3	🟩	🟫	🟨	🟨	🟧
Low 2	🟩	🟫	🟫	🟨	🟨
Very low 1	🟩	🟩	🟩	🟫	🟫 **Scenario 1 DAMAGE**
0	**Very low 1**	**Low 2**	**Average 3**	**High 4**	**Very high 5**

SERIOUSNESS/CONSEQUENCES

The colors green, brown, yellow, orange and red represent risk level (green is very low, brown is low, yeloow is average, orange is high and red is very high)

Note: Risk is determined by the position between the occurrence probability of a hazard/threat and the seriousness of its consequences.

	CALCULATED LEVEL OF RISK	
	LEVEL	SCORE
The calculated risk is 5 (probability 1 x seriousness 5) As a result, there is a LOW OCCURRENCE RISK for the chosen scenario	**Very low**	**1–3**
	Low	**4–6**
	Average	**7–12**
	High	**13–16**
	Very high	**17–25**

The colors green, brown, yellow, orange and red represent risk level (green is very low, brown is low, yeloow is average, orange is high and red is very high)

(d) Risk treatment

With a view to decreasing the risk, measures are required to reduce the following vulnerabilities and/or to improve the following capabilities, according to Table 6.

Table 6. Risk treatment for risk scenario 1.

Vulnerability and/or Capability	Measures Proposed
1. Poor/wrong design of the power substations and overhead powerlines against earthquakes	a. Important investments against earthquakes in the national and European critical infrastructure; b. Predictability of natural disasters (connections with state institutions in the field of emergency situations);
2. Lack of personnel or insufficiently trained personnel for crises, natural calamity, or risk management.	a. Training and refresher courses for operative, maintenance and security personnel; b. Analysis of natural calamity events.

After applying measures to decrease the risk, we obtain the following result, according to Table 7:

Table 7. Measures after risk treatment for risk scenario 1.

Scenario 1: Failure Vulnerability	Identified	After Applying the Measures
1. Poor/wrong design of the power substations and overhead powerlines against earthquakes; 2. Lack of personnel or insufficiently trained personnel for crises, natural calamity, or risk management.	1. Very low	1. Very low
	2. Low	2. Low
	3. Average	3. Average
	4. High	4. High
	5. Very high	5. Very high

(e) Recalculation of the seriousness of the consequences.

Associated Level/Score		Seriousness of Consequences
	1. Very low	The event determines a minor disruption of the activity, without material damages.
	2. Low	The event determines minor material damages and limited disruption of the activity.
	3. Average	Injuries of the personnel and/or certain equipment and utilities losses as well as delays in providing the service.
X	4. High	Serious injuries of the personnel, significant equipment, installations and facilities losses, delays and/or shutting of services.
	5. Very high	Consequences are catastrophic, resulting in deaths and serious injuries of the personnel, important equipment, installations and facilities losses and shutting of the service.

The colors green, brown, yellow, orange and red represent seriousness of consequences level (green is very low, brown is low, yeloow is average, orange is high and red is very high)

(f) Risk level after applying the decrease measures.

PROBABILITY						
	Very high 5	🟫	🟨	🟧	🟥	🟥
	High 4	🟫	🟨	🟨	🟧	🟥
	Average 3	🟩	🟫	🟨	🟨	🟧
	Low 2	🟩	🟫	🟫	🟨	🟨
	Very low 1	🟩	🟩	🟩	Risk scenario 1	
	0	Very low 1	Low 2	Average 3	High 4	Very high 5

SERIOUSNESS/CONSEQUENCES

The colors green, brown, yellow, orange and red represent risk level (green is very low, brown is low, yeloow is average, orange is high and red is very high)

Note: Risk is determined by the position between the occurrence probability of a hazard/threat and the seriousness of its consequences.

	CALCULATED LEVEL OF RISK	
	LEVEL	**SCORE**
The calculated risk is 4 (probability 1 x seriousness 4) As a result, there is a LOW OCCURRENCE RISK for the chosen scenario	**Very low**	**1–3**
	Low	**4–6**
	Average	**7–12**
	High	**13–16**
	Very high	**17–25**

The colors green, brown, yellow, orange and red represent risk level (green is very low, brown is low, yeloow is average, orange is high and red is very high)

B. Risk scenario 2—Terrorist attack → Total/partial shutdown of the national power system.

(a) Settling the probability

With a view to settling occurrence probability, the following probability scale has been adopted:

Associated Level/ScorE	Defining Probability	Periods
1. Very low	The event has a very low occurrence probability. Usual measures for monitoring the evolution of the event are required.	Over 13 years
2. Low	The event has a low occurrence probability. Efforts are required to reduce the probability and/or reduce the impact produced.	10–12 years
X **3. Average**	The event has a significant occurrence probability. Significant efforts are required to reduce the probability and/or reduce the impact produced.	7–9 years
4. High	The event is probable to occur. Priority efforts are required to reduce the probability and attenuate the impact produced.	4–6 years
5. Very high	The event is considered imminent. Immediate and extreme measures are required for protecting the objective and for evacuation to a safe location in the case that the impact requires this.	1–3 years

The colors green, brown, yellow, orange and red represent probability level (green is very low, brown is low, yeloow is average, orange is high and red is very high)

(b) Settling the seriousness of the consequences of the proposed scenario.

The analysis of vulnerabilities and capabilities is displayed in Table 8.

Table 8. Analysis of vulnerabilities and capabilities for risk scenario 2.

Scenario 2: Failure Vulnerabilities and Capabilities	Level
1. Failure to observe fire safety and physical security standards	Very low
	Low
	Average
	High
	Very high
2. Lack of training for personnel dealing with the management of the critical infrastructure protection	Very low
	Low
	Average
	High
	Very high
3. Lack of personnel/insufficient training of cybernetic security personnel. Insecurity of hardware and software systems. Insecure communication. Lack of investments in cybernetic security.	Very low
	Low
	Average
	High
	Very high

Level for vulnerabilities 1, 2, and 3 is very high.

2.4.2. Impact Analysis

We are going to choose the highest of the seriousness impact levels, in accordance with Table 9.

Table 9. Analysis of the impact for risk scenario 2.

Impacts	Level	
1. Huge damages determined by the lack of electric energy	1. Very low	Temporarily
	2. Low	Important damages
	3. Average	Average damages
	4. High	High damages
	5. Very high	Very high damages
2. Huge damage determined by the interdependence with other systems	1. Very low	0–10% of VIC
	2. Low	11–20% of VIC
	3. Average	21–30% of VIC
	4. High	31–40% of VIC
	5. Very high	Over 41% of VIC
3. Potential damage to the environment	1. Very low	0–20%
	2. Low	21–40%
	3. Average	41–60%
	4. High	61–80%
	5. Very high	Over 81%
4. Powerful social impact	1. Very low	0–10% of PC
	2. Low	11–20% of PC
	3. Average	21–30% of PC
	4. High	31–40% of PC
	5. Very high	Over 41% of PC

VIC—Volume of invested capital; PC—Public confidence.

Impacts level for 1, 2, 3, 4, 5 is very high.

Associated Level/Score	Seriousness of Consequences
1. Very low	The event determines a minor disruption of the activity, without material damages.
2. Low	The event determines minor material damages and limited disruption of the activity.
3. Average	Injuries of personnel and/or certain equipment and utilities losses as well as delays in providing the service.
4. High	Serious injuries of the personnel, significant equipment, installations and facilities losses, delays and/or shutting of services.
X 5. Very high	Consequences are catastrophic, resulting in deaths and serious injuries of the personnel, important equipment, installations and facilities losses, and shutting of the service.

The colors green, brown, yellow, orange and red represent seriousness of consequences level (green is very low, brown is low, yeloow is average, orange is high and red is very high)

(c) Calculation of risk level

PROBABILITY	**Very high** **5**	🟫	🟨	🟧	🟥	🟥
	High **4**	🟫	🟨	🟨	🟧	🟥
	Average **3**	🟩	🟫	🟨	🟨	🟧 **Risk scenario 2**
	Low **2**	🟩	🟫	🟫	🟨	🟨
	Very low **1**	🟩	🟩	🟩	🟫	🟫
	0	**Very low** **1**	**Low** **2**	**Average** **3**	**High** **4**	**Very high** **5**
			SERIOUSNESS/CONSEQUENCES			

The colors green, brown, yellow, orange and red represent risk level (green is very low, brown is low, yeloow is average, orange is high and red is very high)

Note: Risk is determined by the position between the occurrence probability of a hazard/threat and the seriousness of its consequences.

	CALCULATED LEVEL OF RISK	
	LEVEL	**SCORE**
The calculated risk is 15 (probability 3 x seriousness 5) As a result, there is a HIGH OCCURRENCE RISK for the chosen scenario	🟩 **Very low**	**1–3**
	🟫 **Low**	**4–6**
	🟨 **Average**	**7–12**
	🟧 **High**	**13–16**
	🟥 **Very high**	**17–25**

The colors green, brown, yellow, orange and red represent risk level (green is very low, brown is low, yeloow is average, orange is high and red is very high)

(d) Risk treatment

With a view to decreasing the risk, measures are required to reduce the following vulnerabilities and/or to improve the following capabilities, according to Table 10.

Table 10. Risk treatment for risk scenario 2.

Vulnerability and/or Capability	Measures Proposed
1. Failure to observe fire safety and physical security standards.	a. Observing and monitoring fire and physical safety standards.
2. Lack of training for personnel dealing with the management of the critical infrastructure protection.	a. Training and refresher courses for personnel dealing with the management of the critical infrastructure protection.
3. Lack of personnel/insufficient training of the cybernetic security personnel. Insecurity of hardware and software systems. Insecure communication. Lack of investments in cybernetic security.	a. Training personnel in cybernetic security. b. Acquiring performing and secured hardware and software systems. c. Major investments in cybernetic security components.

After applying the measures for decreasing the risk, the following result, according to Table 11.

Table 11. Measures after risk treatment for risk scenario 2.

Scenario 2: Failure Vulnerability	Identified	After Applying the Measures
Failure to observe fire safety and physical security standards Lack of training for personnel dealing with the management of critical infrastructure protection -Lack of personnel/insufficient training of the cybernetic security personnel. Insecurity of hardware and software systems. Insecure communication. Lack of investments in cybernetic security.	1. Very low	1. Very low
	2. Low	2. Low
	3. Average	3. Average
	4. High	[✓ 4. High]
	[✓ 5. Very high]	5. Very high

(e) Recalculation of the seriousness of the consequences.

Associated Level/Score		Seriousness of Consequences
	1. Very low	The event determines a minor disruption of the activity, without material damages.
	2. Low	The event determines minor material damages and limited disruption of the activity.
	3. Average	Injuries of personnel and/or certain equipment and utilities losses as well as delays in providing the service.
X	4. High	Serious injuries of personnel, significant equipment, installations and facilities losses, delays and/or shutting of services.
	5. Very high	Consequences are catastrophic, resulting in deaths and serious injuries of the personnel, important equipment, installations and facilities losses and shutting of the service.

The colors green, brown, yellow, orange and red represent seriousness of consequences level (green is very low, brown is low, yeloow is average, orange is high and red is very high)

(f) Risk level after applying the decrease measures

PROBABILITY						
	Very high 5	🟫	🟨	🟧	🟥	🟥
	High 4	🟫	🟨	🟨	🟧	🟥
	Average 3	🟩	🟫	🟨	🟨 Risk scenario 2	🟧
	Low 2	🟩	🟫	🟫	🟨	🟨
	Very low 1	🟩	🟩	🟩	🟫	🟫
	0	Very low 1	Low 2	Average 3	High 4	Very high 5

SERIOUSNESS/CONSEQUENCES

The colors green, brown, yellow, orange and red represent risk level (green is very low, brown is low, yeloow is average, orange is high and red is very high)

Note: Risk is determined by the position between the occurrence probability of a hazard/threat and the seriousness of its consequences.

	CALCULATED RISK LEVEL	
The calculated risk is 12 (probability 3 x seriousness 4) As a result, there is an AVERAGE OCCURRENCE RISK for the chosen scenario	**LEVEL**	**SCORE**
	Very low	**1–3**
	Low	**4–6**
	Average	**7–12**
	High	**13–16**
	Very high	**17–25**
The colors green, brown, yellow, orange and red represent risk level (green is very low, brown is low, yeloow is average, orange is high and red is very high)		

3. Results and Discussion

After assessing the risk scenarios, the results are as follows:

(a) Risk scenario 1—220 kV–750 kV Power substation natural calamity → Blackout;

1. Settling the probability: level/score—1 (stays stable);
2. Settling the seriousness of the consequences: level/score—5;
3. Calculation of the risk level: value 5 → Low risk;
4. Recalculation of the seriousness of the consequences: level/score—4;
5. Recalculation of the risk level: value 4 → Low risk.

Let us notice that after assessing risk scenario 1 (Figure 4), the risk level with a value of 5 (low risk) changes to 4 (low risk).

(b) Risk scenario 2—220 kV–750 kV Power substation terrorist attack → Blackout.

1. Settling the probability: level/score—3 (stays stable);
2. Settling the seriousness of the consequences: level/score—5;
3. Calculation of the risk level: value 15 → High risk;
4. Recalculation of the seriousness of the consequences: level/score—4;
5. Recalculation of the risk level: value 12 → Average risk.

Let us notice that after assessing risk scenario 2 (Figure 5), the risk level with a value of 15 (high risk) changes to 12 (average risk).

The strategy regarding the security of Romania's national power system is displayed in Table 12.

After having carried out the study, we propose the implementation of a management system for the protection and security of Romania's national power system's critical energy infrastructure that is able to provide both continuity of the activities and energy processes and a good technical resilience. The scenarios proposed and the results emerging from the study might represent important references for those responsible for administering, operating, and providing the safety and security of energy critical infrastructures (power plants, power substations, and overhead powerlines) requiring 220 kV, 400 kV, and 750 kV voltages and belonging to the energy systems. The strategic objectives emerging from these scenarios are as follows:

1. Providing a unitary character for the identification, designation, and protection procedures for the national and European energy critical infrastructures;
2. Designing and operationalizing the national system for early warning, through integrating all the existing informational and organizational networks and capabilities;
3. Correctly assessing the level of vulnerability of energy critical infrastructures and identifying the measures required for preventive interventions and decreasing vulnerabilities;
4. Developing national, regional, and international cooperation relations in the domain of the protection and security of energy critical infrastructures.

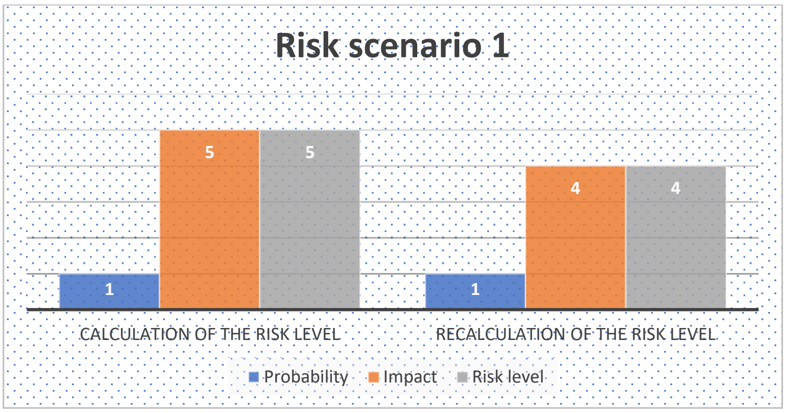

Figure 4. Risk scenario 1.

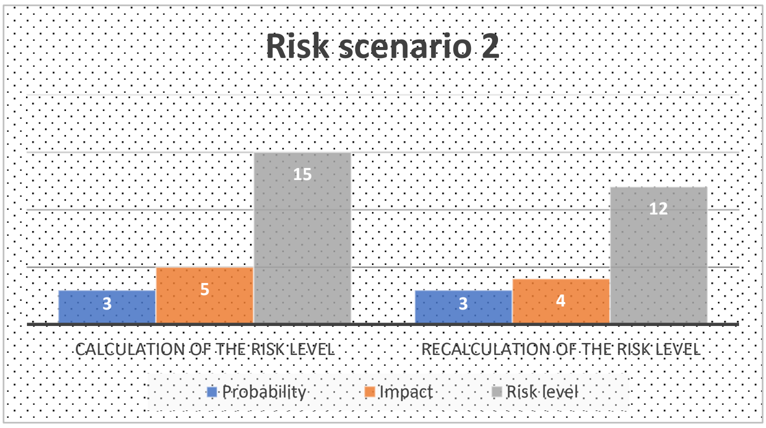

Figure 5. Risk scenario 2.

Table 12. Strategy regarding the security of Romania's national power system resulting from the measures proposed.

Risk Scenario	Vulnerability and/or Capability	Measures Proposed
Risk scenario 1	1. Poor/wrong design of the power stations and aerial electric lines against earthquakes	a. Major investments in the national and European critical infrastructure against earthquakes; b. Predictability of natural disasters (connections with the state institutions in the domain of emergency situations)**.**
	2. Lack of personnel or personnel who are insufficiently trained for crises, natural calamities, or risk management	a. Training and refresher courses for operative, maintenance, and security personnel; b. Analysis of the events that represent natural calamities.
Risk scenario 2	1. Failure to observe fire safety and physical security standards	a. Observing and monitoring fire safety and physical security standards.
	2. Lack of personnel training in the management of the critical infrastructures' protection	a. Training and refresher courses for the personnel dealing with the management of the critical infrastructures' protection.
	3. Lack of personnel/insufficient training of the personnel in cybernetic security. Insecure hardware and software systems. Insecure communication. Lack of investments in cybernetic security.	a. Training the personnel in cybernetic security; b. Acquiring performing and secured hardware and software systems; c. Major investments in cybernetic security components.

4. Conclusions

The assessment of the two risk scenarios for energy critical infrastructures with European connection enables the foundation of a strategy, as a result of the measures proposed for each risk scenario. The measures proposed after the assessment, quantified in an energy security strategy, could represent the security basis for Romania's national power system and, implicitly, for its economic and national security. Through generalization and particularization, this study on Romania's national power system might be adapted to various European states and could set forth possible elements of instability and insecurity quantified by means of vulnerabilities, threats, risks, and dangers. The study also proposes measures for eliminating these instability and insecurity elements, which would result in a power security strategy, matching both the findings of recent studies in the domain and Romania's energy field. The implementation of the proposed model for states within the European Power System ENTSO-E, or the provision of technical, geopolitical, or energy security consulting services, can be executed very simply, by addressing and critically analyzing the identification of all vulnerabilities and risks to national systems by assessing the two risk scenarios from this paper that are effective for each individual state.

So, power substations play a key role in ensuring energy security, being critical nodes in the electricity transmission and distribution network. Their importance can be highlighted by several fundamental aspects:

1. Stability and reliability of the power grid:
   - Power substations ensure the transformation and distribution of electricity at different voltage levels, maintaining the stability of the grid;
   - They allow load balancing and energy flow management to avoid overloads and voltage drops.
2. Integration of renewable energy sources:
   - Power substations are essential for the efficient integration of renewable energy, such as wind farms and photovoltaics;
   - Emphasis on energy conversion and adaptation to grid requirements, contributing to the energy transition.
3. Reduction in the risks of interruptions and damages:
   - By using protective and automation equipment, electrical stations help prevent major damage;
   - Modern power substations have SCADA (Supervisory Control and Data Acquisition) systems that allow real-time monitoring and control, reducing the risk of extended power outages.
4. National energy security:
   - Power substations are critical infrastructures for national security, ensuring the continuity of electricity supply in key sectors such as health, industry, and transport;
   - In the case of unforeseen events (natural disasters, cyber, or physical attacks), well-protected power substations can keep the energy system running.
5. Economic efficiency and loss reduction:
   - The well-equipped power network with modern substations can reduce transmission and distribution losses, which leads to financial savings and more efficient use of energy resources;
   - By upgrading power substations, it improves the performance of the entire energy system, reducing operating and maintenance costs.

In conclusion, power substations are a fundamental pillar of energy security, contributing to the stability, reliability, and efficiency of the energy system. Investments in their modernisation and digitalisation are essential to ensure a safe and sustainable supply of electricity.

Practical Applications and Limitations of Research in the Field of Electricity Crises

Understanding the practical applications and limitations of research in electricity crises is essential for managing this global phenomenon more efficiently.

(a) Practical Applications of Research:
   - Improvement of Smart Grids—Studies help optimize energy distribution through advanced monitoring technologies and automated control systems.
   - Integration of Renewable Sources—Research supports the development of solutions for efficiently integrating solar and wind energy, reducing reliance on fossil fuels.
   - Energy Storage—Advances in batteries and other storage methods (e.g., green hydrogen) are applied to stabilize the power grid.
   - Strategies for Reducing Consumption—Policies and technologies for energy efficiency and demand management are being developed.
   - Backup and Resilience Systems—Research contributes to the creation of infrastructures that better withstand power outages or cyberattacks.

(b) Limitations of Research:
   - High Costs—Developing and implementing innovative solutions require significant investments.
   - Institutional and Political Resistance—The adoption of changes can be hindered by rigid regulations and economic interests.
   - Dependence on Existing Infrastructure—Many power grids are outdated and cannot be modernized quickly.
   - Unpredictability of External Factors—Extreme events (storms, cyberattacks, wars) can affect the effectiveness of proposed solutions.
   - Lack of Data and Predictive Models—Research requires precise data and reliable predictive models to propose effective solutions.

Author Contributions: Conceptualization, N.D.F. and D.C.P.; methodology, D.C.P., N.D.F., G.D.V., M.I.-O., C.I.M., A.N., D.-C.D., A.-M.C. and C.B.; software, D.T. and E.A.C.; validation, N.D.F. and D.C.P.; formal analysis, D.C.P., G.D.V., M.I.-O., A.N., D.-C.D. and C.B.; investigation, D.T.; resources, D.C.P.; data curation, N.D.F. and A.-M.C.; writing—original draft preparation, D.T., E.A.C., C.I.M. and A.-M.C.; writing—review and editing, D.C.P., N.D.F., G.D.V., E.A.C., C.I.M., A.N., D.-C.D., A.-M.C. and C.B.; visualization, D.C.P.; supervision, D.C.P., M.I.-O. and C.B.; project administration, D.C.P.; funding acquisition, D.C.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not require ethical approval.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data is unavailable due to privacy, ethical restrictions.

Conflicts of Interest: No conflict of interest.

References

1. Fita, N.D.; Ilieva Obretenova, M.; Schiopu, A.M. *National Security—Elements Regarding the Optimization of the Energy Sector*; Lambert Academic Publishing: London, UK, 2024.
2. Barb, C.M.; Fita, N.D. A Comparative Analysis of Risk Assessment Techniques from the Risk Management Perspective. In Proceedings of the 9th International Conference on Manufacturing Science and Education—MSE 2019: Trends in New Industrial Revolution, Sibiu, Romania, 5–7 June 2019; Volume 290.
3. Homer-Dixon, T. *The Upside of Down: Catastrophe, Creativity, and the Renewal of Civilization*; Paperback—Illustrated, January 31; Knopf Canada Publisher: Toronto, ON, Canada, 2008.
4. O'Connor, J. *The Fiscal Crisis of the State*; Routledge: New York, NY, USA, 2001.
5. Sabin, P. *The Bet: Paul Ehrlich, Julian Simon, and Our Gamble over Earths*; Yale University Press Publisher: London, UK, 2013.
6. Heinberg, R. *Blackout: Coal, Climate and the Last Energy Crisis*; New Society Publishers: Gabriola Island, BC, Canada, 2009.
7. Gernego, I.; Liakhova, O.; Dyba, M. Crisis management in the energy sector in conditions of increasing epidemiological risks. *Polityka Energetyczna—Energy Policy J.* **2022**, *25*, 25–44. [CrossRef]
8. Glachant, J.-M. *Reforming the EU Internal Electricity Market in the Middle of a Huge Energy Crisis: An Absolute Short-Term Emergency or Preparation for the Future?* Working Paper, EUI RSC, 2023/03; European University Institute: Florence, Italy, 2022; Available online: https://cadmus.eui.eu/handle/1814/73658 (accessed on 29 January 2025).
9. MacKay, D.J.C. *Sustainable Energy—Without the Hot Air*; UIT Cambridge Ltd. Publisher: Cambridge, UK, 2009.
10. Gheorghe, A.; Katina, K. Resilience and Engineering System—Research Trends and Challenges. *Int. J. Crit. Infrastruct.* **2014**, *10*, 193–199.
11. Volkanovski, A.; Čepin, M.; Mavko, B. Application of the Fault Tree Analysis for Assessment of Power System Reliability. *Reliab. Eng. Syst. Saf.* **2009**, *94*, 1116–1127. [CrossRef]
12. Alhelou, H.H.; Hamedani-Golshan, M.E.; Njenda, T.C.; Siano, P. A Survey on Power System Blackout and Cascading Event: Research Motivations and Challenges. *Energies* **2019**, *12*, 682. [CrossRef]
13. Muresan, L. *European Security and Defense Policy—An Element Influencing Romania's Actions in the Field of Security and Defense Policy*; Study no. 4.; European Institute of Romania: Bucharest, Romania, 2004.
14. Petrilean, D.C.; Irimie, S.I. Operational Influence on the Energetic Efficiency of a Gas Cogenerated Operated Electricity Generator. *J. Environ. Prot. Ecol.* **2016**, *17*, 1464–1471.
15. Curt, C.; Tacnet, J.M. *Risk Anal.* **2018**, *38*, 2441–2458. [CrossRef]
16. *European Commission. Commission Staff Working Document Impact Assessment Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities*; European Commission: Brussels, Belgium, 2020.
17. Petrilean, D.C.; Irimie, S.I. Solutions for the capitalization of the energetic potential of sludge collected in Danutoni Wastewater Treatment Plant. *J. Environ. Prot. Ecol.* **2015**, *16*, 1203–1211.
18. Zhang, Y.; Xu, Y.; Dong, Z.Y. Robust Ensemble Data Analytics for Incomplete PMU Measurements-Based Power System Stability Assessment. *IEEE Trans. Power Syst.* **2018**, *33*, 1124–1126.
19. Amini, S.; Pasqualetti, F.; Mohsenian-Rad, H. Dynamic load altering attacks against power system stability: Attack models and protection schemes. *IEEE Trans. Smart Grid* **2018**, *9*, 2862–2872.
20. Ahmad, I.; Khan, F.; Khan, S.; Khan, A.; Tareen, A.W.; Saeed, M. Blackout Avoidance through Intelligent Load Shedding in Modern Electrical Power Utility Network. *J. Appl. Emerg. Sci.* **2018**, *8*, 48–57.

21. Zamani, R.; Hamedani-Golshan, M.E.; Alhelou, H.H.; Siano, P.; Pota, H.R. Islanding detection of synchronous distributed generator based on the active and reactive power control loops. *Energies* **2018**, *11*, 2819. [CrossRef]
22. *ISO 31000:2018*; Risk Management. ISO—International Organization for Standardization: Geneva, Switzerland, 2024.
23. Carreras, B.A.; Reynolds-Barredo, J.M.; Dobson, I.; Newman, D.E. Validating the OPA Cascading Blackout Model on a 19402 Bus Transmission Network with Both Mesh and Tree Structures. In Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS), Wailea, HI, USA, 8–11 January 2019.
24. Xu, D.; Wang, H. Blackout Risk Assessment of Cascading Outages Considering Wind Power Uncertainty. In Proceedings of the 2018 IEEE International Conference on Energy Internet (ICEI), Beijing, China, 21–25 May 2018; pp. 252–257.
25. Liu, B.; Zhou, B.; Jiang, D.; Yu, Z.; Yang, X.; Ma, X. Distributed Accommodation for Distributed Generation–From the View of Power System Blackouts. In *Advances in Green Energy Systems and Smart Grid*; Springer: New York, NY, USA, 2018; pp. 236–246.
26. Ilieva-Obretenova, M. Information System Functions for SmartGrid Management. *Sociol. Study* **2016**, *6*, 96–104. [CrossRef]
27. Vasilescu, G.D.; Petrilean, C.D.; Kovacs, A.; Vasilescu, G.V.; Pasculescu, D.; Ilcea, G.I.; Burduhos-Nergis, D.-P.; Bejinariu, C. Methodology for Assessing the Degree of Occupational Safety Specific to Hydro-Technical Construction Activities, in order to Increase Their Sustainability. *Sustainability* **2021**, *13*, 1105. [CrossRef]

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.