Bulletin of "Carol I" National Defence University
10.53477/2284-9378-22-75

THE RESILIENCE OF CRITICAL INFRASTRUCTURES WITHIN THE NATIONAL ENERGY SYSTEM IN ORDER TO ENSURE ENERGY AND NATIONAL SECURITY

Lect. Eng. Nicolae Daniel FÎȚĂ, PhD*
Prof. Eng. Sorin Mihai RADU, PhD**
Assoc. Prof. Eng. Dragoș PĂSCULESCU, PhD***

Energy security and implicitly the regional energy architecture composed of critical energy infrastructures (power substations and overhead lines at 400 kV), can undergo various mutations and transformations caused by a possible syncope in the extraction, transport and exploitation of energy resources and energy, due to energy dynamism. The vulnerability of these critical energy infrastructures generates a number of risks and threats to them, thus endangering societal life, creating malfunctions and generating extreme damage to the state. Critical energy infrastructures thus become indispensable to society, without which the state and its mechanisms cannot function and ensure societal well-being, and their protection becomes a major national and European objective, prompting representatives of the member states of the European Union to take action to identify and manage any risk or threat. In the face of the vulnerabilities, threats and risks Romania faces in the new dynamic, turbulent and unpredictable geopolitical context of global, regional and Euro-Atlantic security, amid the military and health crisis and amplified by the global energy crisis manifested by the unfounded and unexpected increase in energy price, the Romanian state should have a strategy for strengthening the resilience of critical energy infrastructures, based on predictability, flexibility, continuity, adaptability and resilience.

Keywords: resilience; critical energy infrastructure; national security; black-out.

Introduction

The definition of "black-out electricity": a generalized power failure that manifests itself in the lack of electricity to household, industrial and critical consumers and can cause major national crises with catastrophic and devastating effects, endangering national security and well-being (N. D. Fîță, S. M. Radu, et al. 2021, 37-58).

Since electricity infrastructure (power stations, power substations and overhead lines) ensures access to electricity for the population and national industry, it is critical that all sectors of the national economy are dependent on electricity and that the member states of the European Union are obliged to take action toward identification, designation, analysis, evaluation, their protection and resilience.

***University of Petrosani*
e-mail: *daniel.fita@yahoo.com*
****University of Petrosani*
e-mail: *sorin_mihai_radu@yahoo.com*
*****University of Petrosani*
e-mail: *pdragos_74@yahoo.com*

But these critical power infrastructures vital to everyday life and to ensuring national security can be vulnerable, endangering societal welfare and causing disruption to state mechanisms and citizens.

A possible "black-out" at national level is extremely unlikely, because the National Energy System which is composed of critical energy infrastructures (power stations, power substations and overhead lines) is a fairly safe technical system, and the specialists of the national electricity transmission company Transelectrica SA, the company that manages the proper functioning of the National Energy System in optimal conditions, safety and security, is very well specialized and trained in this field.

However, in the context of the current global energy crisis, amid the unpredictability of the political and legislative system, corruption and incompetence in the National Energy System and lack of investment, a possible black-out must be considered and some calculations can be made, and for this reason, preventing such an undesirable event is imperative and mandatory.

Following the concluding findings on the

National Energy System, it is recognized that an approach to the most appropriate pathways to prevent, reduce, combat and eliminate potential *energy security breaches*[1] involves a deeper and more accurate knowledge and understanding of the underlying reasons behind energy security breaches, which can be perverse, varied and often combined (Fîță, Păsculescu, et al. 2022, 180-201).

The concept of resilience

The concept of resilience has been adopted relatively recently from the study of social sciences, especially from the research of population behavior in crisis situations generated by certain unforeseen events, such as: *natural disasters* (storms, tornadoes, floods, droughts, fires, frost, avalanches, landslides, earthquakes, volcanic eruptions, etc.), *wars* (civil, military, hybrid, etc.), *terrorist risks and threats* (cyber, chemical, biological, ecological, energy, etc.), *internal disturbances* (riots, strikes, revolutions, etc.), *accidents at work* (individual, collective, etc.), *technological events* (incidents, breakdowns, etc.), *psychological trauma* (death, divorce, loss, constraints, etc.), and *epidemics/ pandemics* (natural, artificial, etc.).

The conceptual meanings of resilience are very diverse, being found in areas such as: *sociology, psychology, psychiatry, management, economics, and the economy. Ecology, engineering, cybernetics, etc., and all these definitions are integrated into the science of sustainability* (Bănică and Muntele 2015), and this discipline is characterized by a general approach, with a broad scope of conceptual and applied meanings of sustainability, which integrates ideas and actions from natural, social, engineering, medical, etc., to improve knowledge and action, as well as to create a dynamic link between the components, in order to ensure sustainability (sustainable development), especially social systems. The inclusion of resilience in this complex multidisciplinary science highlights the theoretical and practical role of the concept for the maintenance and development of sustainable systems, and its fundamental characteristic is *to empower the resources and structural components of a societal (social) or physical entity to cope with disruptive changes or actions.*

The U.S. Department of Homeland Security (DHS) believes resilience is the ability of an entity to prepare and adapt to changing conditions, resist and recover quickly from disturbances, deliberate attacks, accidents, incidents, or threats.

Dimensions of resilience: (MCEER 2008):

- *societal (social) resilience:* the ability of society to reduce the impact of a crisis, to adapt by helping the first interveners or those who act as volunteers;
- *economic resilience:* the ability of an entity to cope with the additional costs that arise in a crisis;
- *organizational resilience:* the ability of crisis managers to make decisions and measures that will avoid a crisis or reduce its impact;
- *technical resilience:* the ability of the physical system of the organization to behave appropriately in the event of a crisis.

Properties of resilience:

- *robustness:* the strength or ability of the elements, systems and other units analyzed to withstand a certain level of stress or stress without suffering degradation or loss of functionality;
- *redundancy:* the extent to which elements, systems or other units analyzed capable of meeting functional requirements in the event of disruption, degradation or loss of functionality events;
- *ability to react:* the ability to identify problems, prioritize and mobilize resources when conditions threaten to disrupt some elements, systems or other units analyzed;
- *fast recovery capability:* ability to meet priorities and achieve objectives in a timely manner to limit losses and avoid future disruption.

Resilience and Security:

Resilience has become an indicator of the European Union's security policy, and in this regard, the European Commission has developed the *Action Plan for Resilience in Crisis Countries 2013 – 2020*[2], a new approach has been reached to the societal dimension of national and European

[1] Energy Security Breaches – non-compliance with security prescriptions, generated by critical infrastructures and/or the human factor, followed by technical incidents (isolated/ associated), technical failures (light/serious-black-out) and work accidents within the National Energy System.

[2] Action Plan for Resilience in Crisis Prone Countries 2013 – 2020 – European Commision.

Figure 1 *Sequential cycle critical infrastructures*

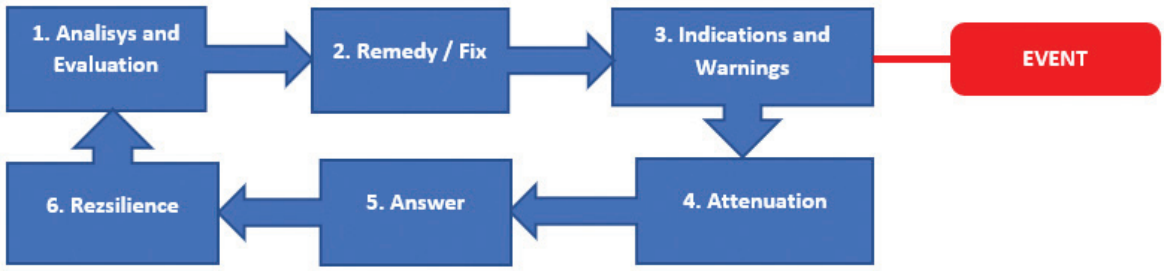

Figure 2 *Closed circuit of critical infrastructures*

security, focusing on the citizen, community and population of a state or region. In the 2012 European Commission (European Commision 2017) Communication on the EU approach to resilience, it is defined as the *ability of an individual, household, community, region or country to resist, to adapt and recover quickly from stress and shock situations.* The EU Global Strategy broadens the definition of this concept and resilience is seen as a broader concept, encompassing all individuals and society as a whole, based on democracy, trust in institutions and sustainable development, and the capacity to reform. The EU's strategic approach to resilience aims to achieve the set of ambitious targets for EU external action in a sustainable manner, reinforcing:

- the adaptability of states, societies, communities and individuals to political, economic, environmental, demographic or societal pressures, in order to further progress toward achieving national development objectives;
- the capacity of a state, faced with significant pressures to build, maintain or restore its essential functions, as well as basic social and political cohesion, in a way that ensures respect for democracy, the rule of law, human rights and fundamental rights that promote security and progress for all in the long term;
- the capacity of societies, communities and individuals to manage opportunities and risks in a peaceful and stable way and to establish, maintain or restore livelihoods in the face of major pressures.

Life cycle of critical energy infrastructures

The Romanian Government mandated the Ministry of Internal Affairs, through the National Center for the Coordination and Protection of Critical Infrastructures – NCCPIC, to coordinate and protect critical infrastructures on Romania's territory. The protection of national critical infrastructures is a complex, multi/inter/trans disciplinary task, involving all sectors of the national economy, defense, intelligence and intervention in case of emergency and necessity, without which the national security and the welfare of the Romanian people would be in great danger. It is assumed and considered to be almost impossible to protect a critical infrastructure 100% regardless of the sector in which it originates, therefore greater importance must be given by state institutions and private companies that are owners, managers or operators of critical infrastructure, through prevention and prevention activity (analysis, evaluation and remediation of the risks and vulnerabilities found) in order to secure them. Particular importance should also be given to mitigation work and the return (technical/societal/human resilience) of critical infrastructure to normality following a negative event.

The sequential cycle and closed circuit of critical infrastructures (N. D. Fîță 2020) are schematized in figures 1 and 2 (Fîță, Radu and Păsculescu 2021).

The six phases of the critical infrastructure lifecycle create a global solution to protect and secure it. Life cycle phases occur before, during and after the event and can compromise, degrade or destroy critical infrastructures

The summary of the six phases is commented on in Table 1:

Description, analysis and quantification of a national power black-out from May 10, 1977

Description of the event

On May 10, 1977, Romania was in the worst power black-out of all time. This lasted between 4 and 5 hours and consisted of a succession of technical incidents amplified by the errors of the dispatching and operating personnel and during this time no domestic or industrial consumers were supplied with electricity, generating huge damages.

Event analysis (sequential scrolling)

Sequential Scrolling
OLD ENERGY EQUIPMENT AND APPLIANCES (lack of investment and refurbishment) + SEQUENCE OF TECHNICAL INCIDENTS + PERSONNEL ERRORS DISPATCH AND OPERATION (lack of specialized personnel) → BLACK-OUT
POWER SUBSTATION (110 kV) → INSULATION DAMAGE → SHORT-CIRCUIT → AUTOMATIC DISCONNECTION OF HYDRO POWER STATION PROTECTION → THERMAL POWER STATION DISCONNECT → POWER DEFICIT OF NATIONAL POWER SYSTEM (MW) → VOLTAGE REDUCTION IN NATIONAL POWER SYSTEM (220 kV and 400 kV electrical network) → OVERLOAD (220 kV electrical network) → NATIONAL POWER SYSTEM SEPARATION → ASYNCHRONOUS OPERATION → OVERHEAD LINES TRIGGER (220 kV and 400 kV) → NORTH ZONE OF NATIONAL POWER SYSTEM DISCONNECT (non-synchronism) / SOUTH ZONE OF NATIONAL POWER SYSTEM DISCONNECT (protections) → TOTAL OUT OF SERVICE OF NATIONAL POWER SYSTEM (black – out) → ENERGY INSECURITY → ECONOMIC INSECURITY → NATIONAL INSECURITY → DAMAGE → INSTABILITY

Event 1:

At around 08:40 a short-circuit in the 110 kV network (Tismana power substation) led to the automatic disconnection of 3 groups from the Porțile de Fier Hydro Power Station (525 MW) and OHL 400 kV Djerdap (325 MW import). In stabilized regime, after the above triggers, at Rovinari Thermal Power Station, personnel disconnected blocks 3 and 4 (290 MW) within a few minutes. As a result, a significant power deficit (1100 MW) occurred in the National Power System, causing sub-state voltage reductions in the 220 kV and 400 kV power networks.

Event 2:

Around 08.45:00 by triggering the 400 kV transversal coupling Sibiu, the power circulation through the 400 kV network to the south-east of the deficient of National Power System is interrupted, redistributing in the 220 kV network and overloading the OHL Luduș – Ungheni – Fântânele, respectively Mintia – Peștiș – Hășdat – Paroseni.

Event 3:

Around 08:47 o'clock the high frequency block coil on the 220 kV OHL Ungheni – Fântânele, that trigger, as a result, the connecting arteries between the north and south, currently in operation (Pestis – Hășdat, Mintia – Timișoara, Arad – Szeged) trigger the overload.

This event leads to the separation of the National Power System

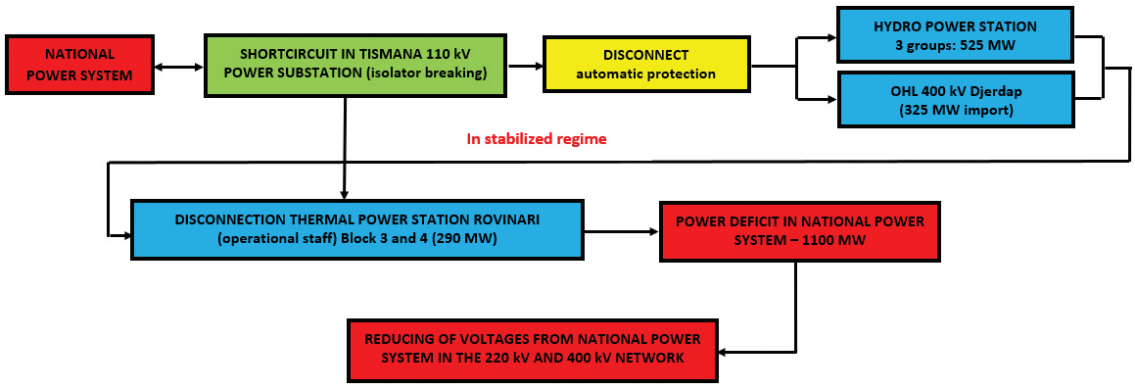

Figure 3 *Technical description – Event 1*

Table no. 1
DESCRIPTION OF LIFE CYCLE PHASES OF CRITICAL INFRASTRUCTURES

Phase number	Phase Name	When it happens	DESCRIPTION
1	**ANALYSIS and EVALUATION**	**Before an event**	- this phase is fundamental and represents the most important stage in the life cycle of a critical infrastructure; - this phase determines their vulnerabilities, dependencies and interdependencies, so that decision makers have all the information they need to make effective choices in managing risks; - following this phase, an assessment of the operational impact of the compromise, degradation or destruction of critical infrastructure is made; - in addition, a cyber attack on these critical infrastructures can be anticipated, as they can be remotely controlled by hackers for destructive or military purposes; - this phase is prevention or self-defense; - critical infrastructures are located in all sectors of the national economy, and each sector is composed of systems, people, programs, equipment or facilities; - critical infrastructures can be simple, such as a facility in a geographical location, or complex, involving geographically dispersed nodes; - the analysis and evaluation consists of 5 stages, which include activities covering all sectors of activity of the national economy and their critical infrastructures: 1) identification of critical infrastructures and elements of criticality; 2) critical infrastructure characterization (association between functions and relationships); 3) analysis of operational impact; 4) vulnerability assessment (probability of natural disasters, criminal or national security events, technological failures); 5) analysis of interdependence.
2	**PREVENTION**	**Before an event**	- during this phase, known weaknesses and vulnerabilities are discussed, where precautions and actions taken before an event are involved, by addressing identified physical or cyber vulnerabilities, hazards and threats that could cause the compromise, degradation or destruction of critical infrastructures; - remediation actions are measures designed to address known virtual and physical vulnerabilities before an event occurs and they can be: • education and awareness about security; • improvement of operational processes; • improvement of system configuration; • system modifications by replacing old, morally and physically worn components with state-of-the-art components with high safety and reliability. - the purpose of the remedy is to improve the reliability and availability of critical infrastructures and applies to any type of vulnerability; - the cost of each remedy depends on the nature of the vulnerability.
3	**INDICATORS of WARNING**	**Before an event** and/or **During an event**	- this phase involves daily monitoring of the critical infrastructure sector to assess insurance and security capabilities and to determine whether there are any event indices to be reported; - the indications are based on information at tactical, operational, theatrical and strategic levels; - at the tactical level, the information comes from the owners of critical infrastructure; - at operational level, the information comes from critical infrastructure sectors; - at the theatrical level, the information comes from regional partners (EU, NATO, allied governments, coalition forces, etc.); - at the strategic level, the information comes from internal and/or external intelligence services, law enforcement and the private sector; - a warning is the process of notifying critical infrastructure owners of a possible threat or danger to them; - indications and warnings are actions that signal an event: probable, planned or ongoing; - where an indication is detected, a warning may be issued to notify all owners or operators of critical infrastructure of a hazard or threat;
4	**ATTENUATION**	**Before an event** and/or **During an event**	- this phase includes prevention (immunization) consolidation actions to prevent the impact resulting from the occurrence of the negative event; - owners or operators of critical infrastructure, regardless of the industrial sector where they are located, take measures to minimize the operational impact of their compromise, degradation or destruction; - the main purpose of the mitigation phase is to minimize the operational impact on other critical infrastructure when critical infrastructure is compromised, degraded or destroyed; - mitigation actions help with phase 5 emergency activities, investigations and management, as well as phase 6 resilience activities.
5	**THE ANSWER**	**After event**	- incident or accident response includes plans and activities undertaken to eliminate the effects or consequences of an event.
6	**RESILIENCE**	**After event**	- this phase involves actions taken to rebuild or rehabilitate critical infrastructure after it has been compromised, degraded or destroyed; - this process is the most challenging and least developed and goes to the owners of critical infrastructure.

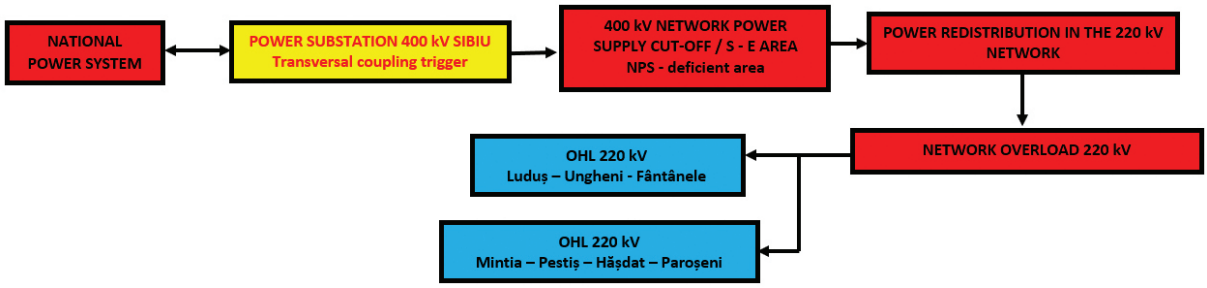

Figure 4 *Technical description – Event 2*

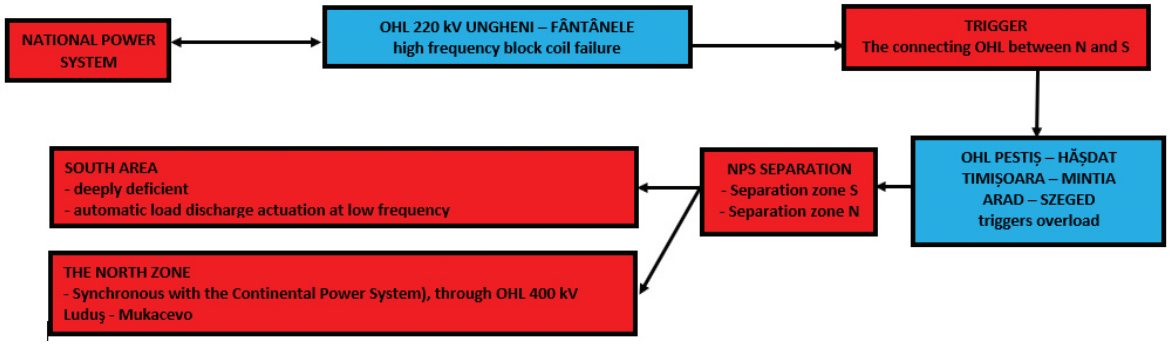

Figure 5 *Technical description – Event 3*

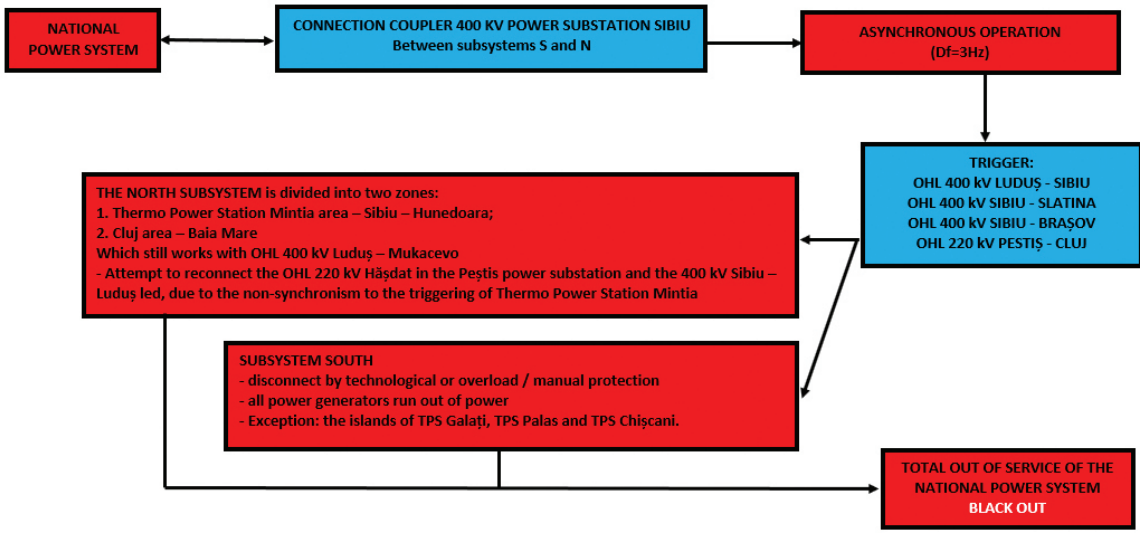

Figure 6 *Technical description – Event 4*

into two areas:

- the south area, deeply deficient, in which automatic discharge of the load acts to decrease the frequency;
- the north area, synchronous with the Continental Power System through the OHL interconnection (400 kV) Ludus – Mukacevo.

Event 4:

Around 08.49 hours, the 400 kV coupler of the 400 kV Sibiu power substation is connected between the mentioned subsystems of the National Power System, operating asynchronously (DF=3Hz). The shock caused by this connection causes the triggering of the 400 kV OHL Luduș – Sibiu, Sibiu – Slatina, Sibiu – Brasov and the OHL 220 kV Pestiș – Cluj. The northern subsystem is divided into two areas: The Thermo power station Mintia area – Sibiu – Hunedoara and the Cluj area – Baia Mare, which still operates with the OHL of interconnection Luduș – Mukacevo. The Southern subsystem, where, within a few minutes, all generating sets have been triggered (by technological or overload protection) or manually disconnected (operating at inappropriate parameters), all power groups are free of tension

(except for the islands of Galati, Palas and Chiscani). In the northern system, the attempt to connect OHL 220 kV Hășdat to the Pestiș power substation and OHL 400 kV Sibiu – Ludus led, due to the non-synchronism, to the triggering of the groups Thermo power station Mintia.

Event 1 + 2 + 3 + 4

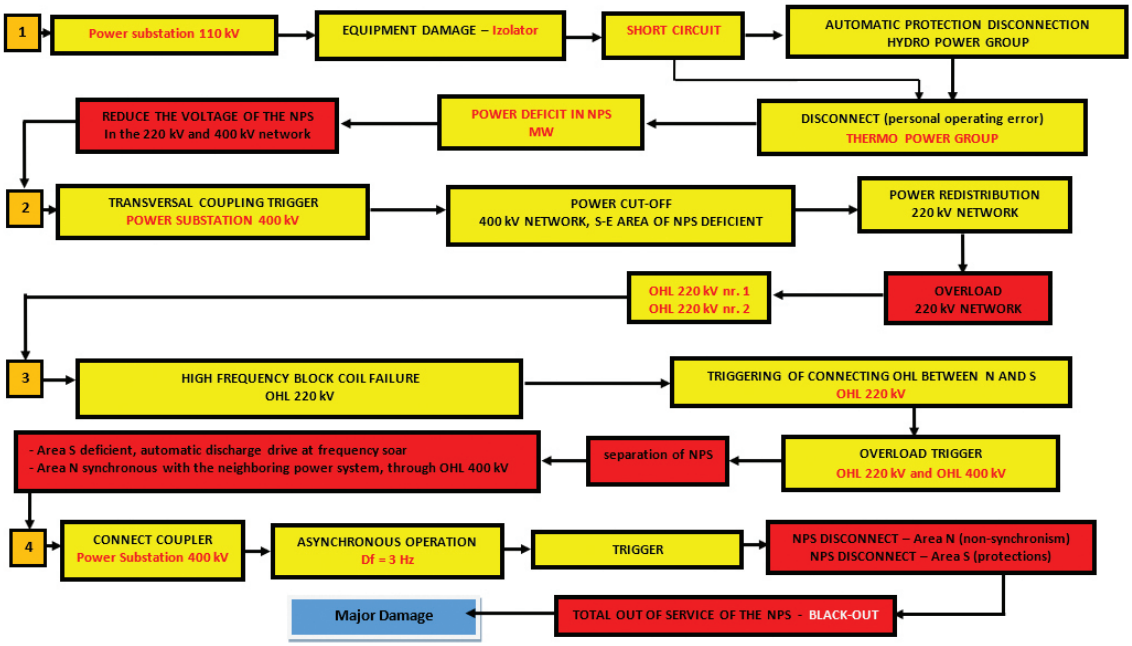

Figure 7 *Technical description – Events 1 + 2 + 3 + 4*

Quantification of the event

The World Bank estimated a damage of about $2 billion, and the analysis was only estimated where a research (study) from Copenhagen Economics was used, based on Eurostat data and electricity prices from 2016, published by the European Commission. This research is about "value of lost – VoLL," which is a cost of energy deprivation, and it is an approximate indicator that takes into account a lot of variables (the time of year or day when the disruption occurs, the extent, how advanced the society is, how energy is consumed, etc.) and in addition there are various ways of calculating this indicator, from country to country. The study calculates the loss in euro/kWh of unconsumed energy for household and commercial consumers, and at European Union level, the results have an extremely high margin, for household consumers ranging from 2 euro/kWh in Bulgaria to 32 euro/kWh in Luxembourg, and for commercial consumers from 11 euro/kWh in Bulgaria to 67 euro/kWh in Ireland. In Romania in 2016 the indicator was 3 euro/kWh for the household consumer and 21 euro/kWh for the commercial consumer (data based on prices and Gross Domestic Product – GDP in 2016) and knowing this data, it was possible to estimate the damage of this unfortunate 6-hour generalized black-out. The average hourly power consumed in Romania was on 23.01.2016 of 8269 MW (average consumption of 8087 MWh), so calculated at an average of six hours, the national consumption was 49614 MWh, i.e. about 50 million kWh. If it is used that the estimate of 28% of consumption is represented by household consumers, their total consumption was 14 million kWh, and the remaining 36 million kWh is counted commercially (this includes the technological own consumption – TOC of the National Power System). If the study values are average, it results in a VoLL of EUR 42 million for the population and EUR 756 million for the industry, so a generalized blackout of electricity nationwide for six hours would bring economic damage (others cannot be counted) of at least EUR 800 million, from the non-use of electricity necessary for economic and domestic activity, and VoLL represents only the economic value of the energy not consumed, not the damage caused by the power supply to the national industry, which are predictable and probably much higher, which cannot be calculated (N. D. Fîță 2019).

Conclusions

A possible and unwanted national black-out brings extreme damage to citizens, society, industry and the national economy, institutions empowered with emergency situations, health care, public order and national security, etc., causing devastating and catastrophic crises that can be detrimental to national security and welfare.

The May 10, 1977 black-out had a domino effect and affected the following critical systems and infrastructures: *the medical system (loss of life), emergency services, police, fire department, ambulance, industrial system (loss of life, large production losses from enterprises, factories, steel plants, mining plants, etc.), livestock farms, drinking water supply system, IT and communications service, oil and gas extraction system, financial-banking system, transport system (airports, train stations, ports, metro, etc.), restaurants, shops,* etc.

The quantification of these damages was estimated only because of the lack of electricity supply to final consumers, not taking into account the interdependencies of all critical systems of the national economy with electricity, which are non-quantifiable.

Such an analysis and assessment of the financial losses caused by an electricity blackout is absolutely necessary to understand the importance of protecting critical energy infrastructures, and in this strategic context, the European Parliament and the European Council issued *Regulation 941/05.06.2019, on risk preparedness in the electricity sector.*

This Regulation lays down rules for cooperation between Member States in order to prevent, prepare for and manage electricity crises, in a spirit of solidarity and transparency, taking full account of the requirements of a competitive internal market in electricity, within ENTSO-E, through the following major actions:

Risk assessment:

- assessment of the risks to the security of supply of electricity;
- the methodology for identifying regional electricity crisis scenarios;
- identification of regional electricity crisis scenarios;
- identification of national electricity crisis scenarios;
- the methodology for short-term and seasonal adequacy assessments;
- short-term and seasonal adequacy assessments.

Risk preparedness plans:

- the establishment of risk preparation plans;
- the content of risk preparedness plans with regard to national measures;
- the content of risk preparedness plans with regard to regional and bilateral measures;
- assessment of risk preparedness plans.

Power crisis management:

- early warning and declaration of an electricity crisis;
- cooperation and assistance;
- compliance with market rules.

Evaluation and monitoring:

- ex post evaluation;
- monitoring;
- handling of confidential information.

BIBLIOGRAPHY

Bănică, Alexandru, and Ionel Muntele. 2015. *Reziliență și teritoriu – operaționalizare conceptuală și perspective metodologice.* Iași: Terra Nostra.

European Commision. 2017. „Comunicare comună către Parlamentul European și Consiliu." *O abordare strategică privind reziliența în cadrul acțiunii externe a UE.* http://www.cdep.ro/eu/examinare_pck.fisa_examinare?eid=528.

Fîță, Daniel Nicolae, Mihai Sorin Radu, and Dragoș Păsculescu. 2021. *Asigurarea, controlul și stabilitatea securității energetice în contextul creșterii securității industriale și naționale.* Petroșani: Universitas.

Fîță, Nicolae Daniel. 2020. *Cercetări privind identificarea vulnerabilităților infrastructurilor critice din cadrul Sistemului Electroenergetic Național de ultra și foarte înaltă tensiune cu conexiune internațională.* Teză de doctorat. Petroșani: Universitatea din Petroșani.

—. 2019. *Identificarea vulnerabilităților infrastructurilor critice din cadrul Sistemului electroenergetic național în contextul creșterii securității energetice.* Petroșani: Universitas.

Fîță, Nicolae Daniel, Dragoș Păsculescu, Cristina Pupăză, and Emilia Grigorie. 2022. „Metodologia de identificare, desemnare, analiză, evaluare, protecție și reziliență a infrastructurilor critice electroenergetice." In *Managementul rezilienței în societatea contemporană*, by Olga Maria Cristina Bucovețchi (coordonatori) Diana Elena Ranf, 180-201. Sibiu: Academiei Forțelor Terestre „Nicolae Bălcescu".

Fîță, Nicolae Daniel, Sorin Mihai Radu, Dragoș Păsculescu, and Emilia Grigorie. 2021. „Abordarea infrastructurilor critice energetice naționale corelată rezilienței societale și sustenabilității." In *Managementul sustenabilității și sustenabilitatea managerială între paradigme clasice și moderne*, by Olga Maria Cristina Bucovețchi, Dorel Badea (coordonatori) Diana Elena Ranf, 37-58. Sibiu: Academiei Forțelor Terestre „Nicolae Bălcescu".

MCEER. 2008. *Earthquake Engineering to Extreme Event – University at Buffalo.* http://www.buffalo.edu/mceer.