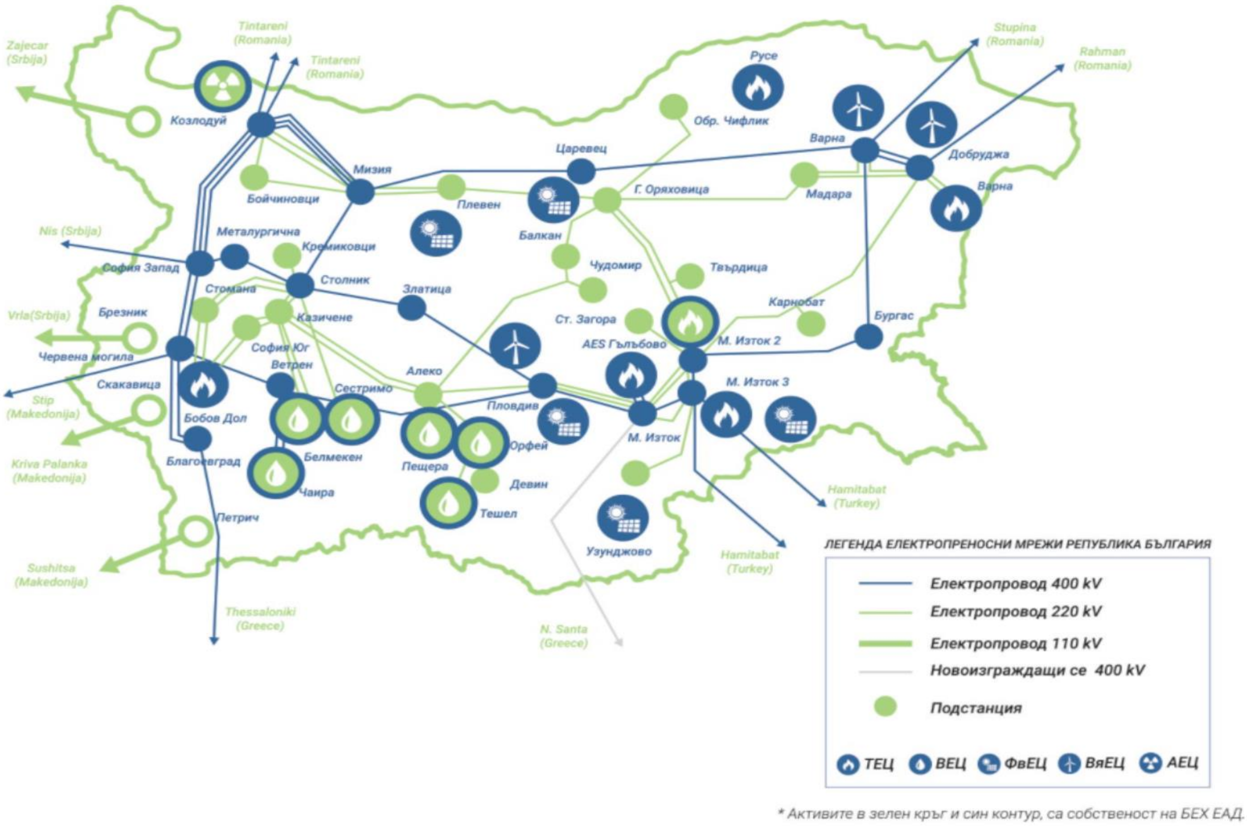
REPUBLIC OF BULGARIA

MINISTRY OF ENERGY

NATIONAL ACTION PLAN
FOR RISK-PREPAREDNESS IN THE ELECTRICITY SECTOR OF THE REPUBLIC OF BULGARIA



SOFIA 2021

CONTENTS:

LIST OF ACRONYMS USED

NPP	Nuclear power plant
GIO	Generation island operation
ALS	Automatic load-shedding
ADCS	Automated Dispatching Control System
ALT	Automatic Load Transfer
AR	Autoreclosures
OSPS	Overvoltage SPS
HPP	Hydro Power Plant
RES	Renewable energy source
GSPP	Gas-steam power plant
DTS	Dispatcher training simulator
SANS	State Agency “National Security”
EC	European Commission
ESO	Electricity System Operator
EPS	Electric Power System
EU	European Union
EDC	Electricity distribution company
EDN	Electricity distribution network
ENTSO-E	European Network of Transmission System Operators - Electricity
ICT	Information and telecommunication technology
EWRC	Energy and Water Regulatory Commission
ME	Ministry of Energy
MIA	Ministry of Internal Affairs
NEK	Natsionalna Elektricheska Kompania (National Electricity Company)
NDPS	National Disaster Protection Staff
DSO	Distribution system operator
TSO	Transmission system operator
ESP	Essential service operators
PsHPP	Pump-storage hydro power plant
FSPP	Fire Safety and Protection of the Population
REPSC	Rules for electric power system control
CMD	Council of Ministers’ decree
SDU	Specialised dispatching units
TPP	Thermal Power Plant
TDC	Territorial Dispatching Center
TS	Transformer station
NDC	National Dispatching Center
SIAP	Staff for the Implementation of the Action Plan
SCADA/EMS	Supervisory Control and Data Acquisition System/Energy Management System

BACKGROUND

Pursuant to article 10 of the Regulation (EU) 2019/941 on establishing "Risk-preparedness plan" in the electricity sector (Regulation (EU) 2019/941), working group determined by order no. Е-РД-16-580/23.08.2021 of the minister of energy developed Risk-preparedness plan in the electricity sector of Bulgaria (the "Plan"). The plan consists of set of crisis scenarios developed under article 7 of Regulation (EU) 2019/941, and namely 14 scenarios falling in 7 categories: Cyberattack, physical attack, insider threat, natural disasters and extreme weather conditions, technical breakdown, fuel shortages and political crises. All of these scenarios are related to events that occur with relatively short notice periods.

The Risk Preparedness Plan in the Electricity Sector contained in this document sets out the procedures to be followed by the actors in the electricity sector during crisis situations, such as those described in the scenarios, in order to minimize disruption caused by to the customers. The plan also covers preventive and mitigation measures that need to be taken to help avoid crises. The roles of the various stakeholders, the communication procedures and the schedule for regular testing of the system are also included in the plan. The key procedures to be applied in such crises are set out in detail in the System Defence Plan and the System Restoration Plan.

In addition to the general preventive and preparatory measures taken to avoid or prepare for a crisis, such as network development plans, there are many other special measures related to the different types of crisis scenarios. These measures include the preparation made in view of the possibility of extreme weather conditions and the annual Winter Outlook Report (WOR) prepared by ENTSO-E; cybersecurity safeguards; technical and infrastructure maintenance standards. The plan contains summaries of the types of measures currently applied in the Bulgarian electricity system. The general approach to consumption management and the rotational disconnection of loads that can be used to prevent or during a crisis event is also presented.

Regulation (EU) 2019/941 sets out requirements for each EU Member State to ensure that there are consistent plans in place to prevent, prepare for and manage crisis events that could lead to outages of power supply. These events may include, for example, extreme weather conditions or technical damage.

As part of the work required under Regulation (EU) 2019/941, the Ministry of Energy is cooperating with ESO EAD to develop a set of potential "crisis" scenarios, as well as with the electricity distribution companies (EDCs) where electricity supply outage is possible in the Republic Bulgaria, and to assess the level of risk associated with each scenario. The scenarios focus on events that occur relatively suddenly and for which the system must be prepared.

It should be noted that in the framework of its daily function to ensure security of supply in Bulgaria, the transmission system operator already has specific procedures in place for dealing with emergencies, and the plans presented here are largely based on existing measures. The purpose of this specific plan is to meet the requirements of the cited Regulation (EU) 2019/941; to bring this information into a uniform European format so that potential crisis scenarios at national and regional level can be identified, assessed and subsequently managed in an improved and coordinated way.

EDCs perform all measures and procedures related to the organization and management of the processes of electricity supply to customers connected to the electricity distribution network (EDN).

These companies interact with all other entities in the field of energy according to pre-regulated protocols or on the basis of legislative documents. Interacts with the Ministry of Energy, EWRC, ESO, NEK - HPPs, RES producers connected to the electricity distribution network.

In the event of crises, they act with pre-prepared structures which are activated and work to solve the challenges. The main principles are occupational safety and minimizing the number and duration of outages in the power supply to customers.

In case of high escalation of incidents above the capacity of an EDC, a memorandum of mutual assistance with the other EDCs on the territory of the country enters into force. Interaction with the Fire Safety and Protection of the Population structures and the Regional/municipal management structures.

1. National electricity crisis scenarios

In accordance with Article 7 of the Risk Preparedness Regulation (EU 2019/941), the Bulgarian competent authority, namely the Minister of Energy, identified 14 relevant national electricity crisis scenarios after consulting the relevant stakeholders and taking into account the regional electricity crisis scenarios identified in the ENTSO-E reports and methodology for identifying regional electricity crisis scenarios.

The identification of national electricity crisis scenarios is based on a proposal discussed in the Stakeholder Risk Preparedness Working Group which was set up specifically for the strict implementation of the Risk Preparedness Regulation. The working group is composed of the relevant stakeholders in accordance with Article 7 (2) of the Risk Preparedness Regulation.

In accordance with Article 7 (3) of the Risk Preparedness Regulation concerning the identification of national electricity crisis scenarios, corresponding to the regional electricity crisis scenarios, 31 ENTSO-E regional electricity crisis scenarios were taken into account.

The scenarios identified with the above documents and analyses were further assessed on the basis of their relevance to the security of electricity supply. In order to establish their relevance, their national risk profile was taken into account. The allocation methodology for identification of the national risk profile is based on the ENTSO-E methodology in accordance with Article 5 of the Risk Preparedness Regulation. This means that each scenario was assessed on the basis of its probability and its possible impact on the security of electricity supply. The probability, as described for the different scenarios, is actually the probability that the scenario will actually occur and lead to an electricity crisis. For example, in the case of a cold front scenario, the probability is not limited to the probability that a cold wave will occur, but considers the probability that this cold wave will occur and lead to an electricity crisis. In order to assess this probability, the sum of the probability of the actual event and the TSO's assessment of the probability of this event leading to a power supply crisis is taken into account. In order to identify the final national electricity crisis scenarios, the following conditions were taken into account:

- Scenarios with high impact on the electricity system and low to medium probability of realization;
- Scenarios that have a relatively high probability of occurrence, but with little or limited impact on the electricity system operation.

Taking into account the methodology presented above, the competent authority decided on the 14 national electricity crisis scenarios, as described in the table below.

1 Risk group	No.	Scenario
Cyberattack	1	Cyberattack against critical ICT business infrastructure of sites directly connected to the electricity network such as TSO, power plant or industrial load

Physical attack	2a	Physical attack on critical assets
	2b	Physical attack on dispatching centers
Insider threat	3	Insider attack, sabotage
Natural disaster and extreme weather conditions	4	Storm
	5	Cold front
	6	Heavy rainfall and flooding
	7	Dry period and hot wave
	8	Wildfire
	9	Earthquake
	10	Pandemic
Technical failure	11	Failure of ICT systems and public telecommunications
	12	Unintentional tripping of an element of system importance due to human error
Fuel shortage	13a	Fossil fuel shortage
	13b	Nuclear fuel shortage
Political	14	War / civil war

1.1 Cyberattack against critical business infrastructure

Risk profile		**Impact**	**Probability**	**Cross-border impact**
High		Critical	Unlikely	High

Information-communication and technological (ICT) systems are subject to increased threats from incidents or malicious attacks that threaten the confidentiality, integrity and accessibility/availability of individual systems. Actions to intentionally stop or obstruct the functioning of an information system by improperly entering, transmitting, deleting, damaging, degrading, altering, hiding or providing restricted digital data in an information system are defined as cyberattacks.

1.1.1 The principle obstruction of ICT services is divided into:

A. Fault (accident, incident)

Obstruction or interruption of operation by an event that is eliminated during normal working hours by operational measures.

B. Emergency

Obstruction or interruption of operation by an event that requires immediate action and poses an immediate danger to people and property.

In case of emergencies, it must be specified in which situations (respectively in case of fault) the authorities must be informed. External support staff may be needed to deal with the emergency. Even if the danger of an emergency is great, it remains an isolated event, localized and without dynamics.

C. Crisis

A crisis is an intertwining or simultaneous occurrence of faults or extraordinary circumstances that cannot be managed with current operational means. A sign of the crisis is its independent expansion, which in case of inaction leads to enormous damage. It is not localized and the extent and time range cannot be estimated. The effects of the crisis threaten society, property and the activities of companies in the energy sector.

D. Disaster

A disaster is declared by the authorities within the meaning of the Disaster Protection Act. In the event of a disaster, the action leader must follow the regulations of the authorities or the crisis manager appointed by them.

1.1.2 The following approaches are applicable:

A. Time requirements

The relevant ISO27000 standard specifies the requirements as follows:
Recovery Time Objective (RTO) means the maximum tolerated time to restart after stopping IT services
Recovery Point Objective (RPO) means the maximum allowable data loss since the last backup.

B. Data recovery

RPO (Recovery Point Objective) regulates the moment from which data should be recovered. This means that the loss of data between the last back-up and the occurrence of a fault is defined by the RPO as an "acceptable loss".

C. Analysis and assessment of crisis management

Once an emergency has been addressed and the escalation has been reduced, it needs to be analysed so that remedial action can be taken on the basis of the identified vulnerabilities.

When addressing an emergency, it may become clear that improvements are needed in organizational structures, ICT or work processes. In such cases, suggestions for improvement should be developed with the competent person in the relevant field.

Each incident must be reported immediately by the incident handler and documented upon completion of the disaster recovery process.

D. Employee participation and training

Training, upskilling, protection measures and regular exercise are important parts of the preventive measures of the emergency management system.

The employees' training in emergency management is guided by the requirements of standards and regulations and is carried out with the help of external consultants, if necessary. The training is carried out at levels (managers, crisis management, specialized staff, other support staff, etc.).

E. External service providers.

Service Level Agreements (SLAs) with critical providers and service providers should be defined, administered and kept by those responsible for the relevant systems/applications.

A likely cyberattack on business-critical infrastructure of sites such as transmission system operators, distribution system operators, power plants and/or large industrial loads that are physically connected to the electricity transmission network would target critical ICT systems for the above purposes. Forms of hacktivism, serious cybercrime, cyber threats from another country, cyberattacks initiated by a third party, or cyberattacks from other individuals or groups of people are considered as part of this scenario. In practice, this means that the person or group of people who attack are able to manipulate ICT systems from inside. In addition, the attacker may be able to complicate the recovery process by blocking users of the attacked systems.

Assuming that the attacker(s) are targeting several systems simultaneously, the scenario is given an overall high risk profile, taking into account its high risk of cross-border impact. By probabilistic calculation, the probability of the scenario is assessed as unlikely, but with a possible impact defined as critical. The low probability is due to the fact that the vital ICT infrastructure of the transmission electricity operators and distribution electricity operators in Bulgaria is very well protected and completely isolated from external access (no internet connection). However, it is important to note that both national and cross-border impacts will highly depend on the severity and duration of the attack. For cross-border implications, this means, for example, that when the ICT systems of neighbouring TSOs are affected, mutual assistance will not be possible. In addition, if the cyberattack cannot be countered quickly enough, it can lead to a power supply outage.

In case of a cyberattack, it is registered and acted upon in accordance with pre-approved and agreed protocols and measures are taken to limit the impact on the systems. The State e-Government Agency (SEGA) is informed according to the pre-determined deadlines and communication channels.

In case of escalation, CSIRT at the Ministry of Energy is activated and it directs the actions of all affected companies in the energy sector.

1.2 Physical attack

The physical attack scenario is divided into two sub-scenarios based on the target of the attack, namely critical assets or dispatching centers.

1.2.1 Physical attack on critical assets

Risk profile	Impact	Probability	Cross-border impact
High	Critical	Unlikely	High

The scenario involving a physical attack on critical assets includes a violent attack on power lines, transformers, substations, power plants and/or data centers. Violent attacks can be implemented in a variety of ways, from drone attacks, hostage-taking, use of explosives or other explosive devices, to attempted sabotage of physical infrastructure.

The scenario has an overall high risk profile with a high risk of cross-border impact. By probability calculation, the probability is assessed as unlikely, and the impact - as critical. In particular, this means that cross-border power exchange, reserve sharing and assistance can be seriously jeopardized if components of the interconnected network infrastructure are also damaged. In combination with adverse conditions, such as adequacy problems, this can lead to automatic tripping of loads. The impact on the electricity system operation depends on the amplitude, severity and whether the attacks are single or multiple and carried out simultaneously. In the worst case, when several critical network components are destroyed in parallel and their recovery can take a long time, the security of supply to a large number of network users can be seriously compromised over a longer period.

Physical impact on electricity system elements cannot have high impact on the Critical Infrastructure, but it is important to ensure the power supply of critical infrastructure facilities by implementing the required measures to increase the category of power supply.

1.2.2 Physical attack on dispatching centers

Risk profile	Impact	Probability	Cross-border impact
High	Critical	Unlikely	High

The risk of attack on the dispatching centers is minimized, given the measures taken by ESO EAD and EDCs to protect them. They are included in the list of strategic sites under CMD 181/2009.

In this way, they fall under the special supervision of the security authorities. The necessary technical and organizational measures have been implemented in accordance with the requirements to strategic sites and the prescriptions of the Ministry of Interior and the State Agency for National Security. They interact with energy sector companies and warn of risks to a particular area or sites.

The scenario related to a physical attack on dispatching centers includes a violent attack targeting the central control sites of transmission system operators, distribution system operators or large power plants, as well as their back-up facilities. The violent attack can be implemented in various ways - from a drone attack, hostage-taking, the use of explosive devices or an attempt to sabotage the centers' operation.

The scenario has an overall high risk profile with a high risk of cross-border impact. By probability calculation, the probability is assessed as unlikely, and the impact - as critical. However, the impact depends on the amplitude of the attack and on whether several dispatching centers are under attack at the same time. For example, if several dispatching centers are attacked at the same time, the power system will be put outside the admissible operating parameters for a short time. In case the attack succeeds to affect only one center, the back-up dispatching units can take control, which ensures that the attack will have a relatively small impact. Bulgaria has a back-up control center of NDC which has the required procedures in crisis situations.

1.3 Insider attack, sabotage

Risk profile	Impact	Probability	Cross-border impact
High	Catastrophic	Unlikely	High

An insider attack scenario involves deliberate sabotage by an employee or subcontractor, possibly initiated by a third party, group, state or other individuals. The attacker can target the physical infrastructure, the virtual infrastructure, or both. In addition to attempting to sabotage, the attacker may try to blackmail key employees or take those employees hostage during the attack.

The scenario has a serious risk profile with a high risk of cross-border impact. By probabilistic calculation, the occurrence of the scenario is considered unlikely. At the same time, if the scenario is materialised, the probability calculation shows that the impact will be catastrophic. A person with detailed knowledge of the operating modes of the power system is able to inflict devastating damage in a short time, including system splitting, power supply outages in large areas, damage to basic equipment, which events require significant time to restore the power system back to normal operation. For example, if the attack disrupts the grid, cross-border energy exchanges, sharing reserves and providing assistance may become impossible for a long period of time. If the insider attack is targeted at taking hostages instead of attacking the physical or virtual infrastructure, the recovery of the system can begin as soon as the hostage crisis is over, without the need to repair the infrastructure.

EDCs has also taken the necessary organizational actions to minimize this type of impact. All administrative buildings have security guards, and specific centers are equipped with panic buttons to quickly inform the security companies or structures of the Ministry of Interior.

1.4 Storm

Risk profile	Impact	Probability	Cross-border impact
High	Limited	Unlikely	High

The initial conditions of this scenario include a storm with an expected wind speed of over 100 km/h, combined with wind gusts of over 150 km/h. The consequences of such extremely strong gusts of wind can seriously affect the components of the electrical infrastructure. In addition, the flow on some interconnections may be disrupted or even interrupted if specific network components are damaged due to the effects of the storm.

The scenario has a high risk profile and a high risk of cross-border impact. The prevailing temperate-continental climate in the country and the analysis of statistical data show that the occurrence of the scenario can be considered unlikely, with an assessment of a significant impact on the security of electricity supply. The stronger the wind speed and gusts, the higher the risk that certain elements of the network will not be able to be used. And although the storm is usually more local in nature, the impact on the network can be quite significant.

At the same time, the scenario could have an impact on the national network. During the last 70 years, the high voltage network in Bulgaria (110 -400 kV) has been built in accordance with the applicable rules in the year of their construction. The applicable rules have been amended in recent years, which means that not all components are built with the same level of resilience. The most likely consequence and impact of a storm with such extreme wind speed will be the disruption of the network integrity which will affect end-users.

1.5 Cold front

Risk profile	Impact	Probability	Cross-border impact
High	Critical	Possible	High

The cold front scenario includes a long period of low temperatures below 0 ℃ (reaching below - 20 ℃ and below) which lead to record levels of electricity consumption. The climate region in which Bulgaria falls, and the Balkan Peninsula as a whole, is characterized by abnormally low temperatures in winter from minus 25 to minus 30 ℃. In the presence of strong winds and snowfall, such record low temperatures cause various accidents (mechanical damage due to icing of overhead power lines, forced downtime of generating capacity) and crisis situations. Such conditions can cause many network components to drop out unexpectedly within a relatively short period of time. This can lead to both adequacy issues due to the extremely high loads in combination with the lack of generating capacity and problems with the network transmission capacity due to failed network components.

The scenario has a "high" risk profile and a high risk of cross-border impact. Based on statistics, the scenario is assessed as possible, with a probabilistic assessment of high impact. The impact of the scenario on the power system may be limited by the introduction of rotational power outages to unprivileged consumers.

1.6 Heavy rainfall and flooding

Risk profile	Impact	Probability	Cross-border impact
High	Limited	Possible	High

Floods are common natural disasters on the territory of the Republic of Bulgaria which cause enormous damage, as they affect urbanized and arable land and can destroy elements of the electricity transmission and distribution system. The main causes of floods are again climate change leading to heavy rains and snow accompanied by unexpectedly strong increases in river inflows, bottle-necks, extensive spills, winds in estuaries, destruction of dikes, dam walls and tailing pond walls, threatening electricity infrastructure.

The heavy rainfall and floods scenario includes prolonged heavy rainfall in combination with a spring wave, which in turn causes floods in large parts of the country. Floods in certain areas can lead to inaccessibility to electricity generation, transmission and distribution infrastructure. This lack of access can disrupt the integrity of the network which will affect end users.

The scenario has a "high" risk profile, with a high risk of cross-border impact. The statistical data show that the probability of the scenario is possible, and its impact on the power system is assessed as limited - due to the local nature of these events in Bulgaria. The impact could be much greater, depending on the location of the floods and whether it will remain local or will affect the electricity generation, transmission and distribution infrastructure in several areas.

1.7 Dry period and hot wave

Risk profile	Impact	Probability	Cross-border impact
High	High	Possible	High

This scenario is associated with dry weather in combination with hot wave, characterized by a duration of at least 10 days, combined with little or no precipitation, with average temperatures above 27 ℃ and expected maximum temperatures of 37 ℃ and more. These hot waves are expected to increase in the future precisely because of climate change.

Extremely high temperatures and lack of rainfall can lead to accidents due to thermal expansion of the conductors (increased sag), overheating of transformers and lowering the water level in major dams for electricity generation. These failures of multiple network elements can occur almost simultaneously in a relatively short period of time which can drastically aggravate the situation. Numerous failures of network components are beginning to affect available reserves, flows to neighbouring countries and supplies to the end user. In addition, dry and hot wave leads to a reduction in the generation levels of several thermal power plants or to their complete shutdown due to insufficient quantity or increased temperature of the cooling water.

However, it should be taken into account that Bulgaria is a country with a clear peak load in the winter and possible unplanned downtime and damage to infrastructure would not affect as strongly as during a cold front in the winter. The difference between the registered peak loads in winter and in summer in the last 20 years for the country is 2464 MW in predominance for winter load. Therefore, the impact of this risk on the power system is assessed as "high" and not as "critical".

1.8 Wildfire

Risk profile	Impact	Probability	Cross-border impact
High	Limited	Very likely	Not significant

On the territory of the Republic of Bulgaria, every year there are forest fires of different intensity which cause loss of human and material resources and endanger mostly the open infrastructure (overhead power lines and substations) of the power system outside the urban environment. The analysis of possible events shows that their occurrence will lead to serious difficulties in the normal operation of the infrastructure in disaster areas. The changes in the country's climate in recent years are increasingly complicating the fire situation, especially in periods of high outdoor temperatures and prolonged summer droughts in large fields, semi-mountainous and some mountainous areas, which significantly increases external risks to the transmission and distribution system.

This risk, although highly likely to materialize, has a limited impact on the power system and cross-border electricity flows due mainly to the local nature of forest fires in Bulgaria and their occurrence mainly during the summer. However, depending on the intensity, such a disaster can have a devastating effect on the electricity infrastructure on a large area, which is why the risk profile is left as "high".

1.9 Earthquake

Risk profile	Impact	Probability	Cross-border impact
High	High	Unlikely	Minor

Earthquakes are natural disasters with the highest degree of danger, which can cause landslides, floods, accidents, epidemics, disruption of communication and transport links, etc. As a result of the displacement of the earth layers, it is possible to break power lines and damage facilities and buildings, which could lead to power outages in certain areas and danger of explosions and fires accompanied by loss of life.

A large part of the electricity transmission network falls into earthquake zones with increased activity which also poses a risk with a high risk profile, which may have a significant impact on the power system, although unlikely as an event and relatively low impact on cross-border electricity flows.

1.10 Pandemic

Risk profile	Impact	Probability	Cross-border impact
Minimal	Minimal	Possible	Not significant

The scenario consists of a virus that is spreading internationally and even globally. The degree of this risk depends on whether it occurs alone or in combination with some of the other risks listed. The pandemic affects all sectors of public life, including social and economic. It is directly dependent on the intensity, territorial scope and duration of the infection. Although the current Covid-19 pandemic has not had serious consequences for security of electricity supply, it cannot be ruled out that a virus with a different profile would pose serious challenges. The risk consists mainly of staff shortages and restrictions on the movement of people, for example as part of measures to limit the spread which can lead for example to delays in the maintenance and repair of facilities and curtailments in the supply chain.

Taking into account the different aspects, the scenario has an overall "minimal" risk profile, with insignificant cross-border impact. It is considered that mutual assistance between TSOs will not be severely limited. Probability based on statistics is considered possible, with a probabilistic impact assessment being minimal.

1.11 Failure of ICT systems and public telecommunications

Risk profile	Impact	Probability	Cross-border impact
High	Critical	Unlikely	High

This scenario involves the unavailability of a large part of the telecommunication infrastructure used to manage the electricity market and/or the electricity system in real time. It may also include the inaccessibility of ICT systems which are crucial for the short-term planning of the power system. The failure of the above-mentioned systems is most often caused by technical failures.

The scenario has a "high" overall risk profile and an assessment for high cross-border impact. The severity of the scenario strongly depends on the scale of the technical damage, the types of systems affected and the duration of the damage. In the event that, for example, the control of the power system in real time cannot be restored quickly enough, the power supply may be interrupted. If the ICT systems of neighbouring TSOs are also affected, it will not be possible to provide mutual assistance. However, SCADA/EMS systems of the different TSOs are in most cases developed by different manufacturers. This reduces the risk of total simultaneous damage.

Given the above conditions, the impact of the scenario is probabilistic considered to be critical. According to statistics, the scenario is unlikely to materialize.

1.12 Unintentional tripping of an element of system importance due to human error

Risk profile	Impact	Probability	Cross-border impact
Minimal	High	Unlikely	High

Although the operational and repair personnel in the electricity sites work according to regulations, rules and instructions, the possibility of human error cannot be excluded. It is possible that a mistake made by the operating and repair personnel will cause cascading tripping of equipment. Cross-border power exchange, reserve sharing and/or mutual assistance may become impossible if overhead power lines between Bulgaria and some of its neighbouring countries or infrastructure near the border are affected.

The human error scenario has an overall insignificant risk profile, with the potential for high cross-border impact. Statistics show that the scenario is unlikely to materialise, but if it does, the probability calculation shows that this scenario would have a high impact.

1.13 Fuel shortage

The scenario of possible fuel shortage is divided into two sub-scenarios based on the type of fuel, namely fossil fuels and nuclear fuel.

1.13.1 Fossil fuel shortage

Risk profile	Impact	Probability	Cross-border impact
Minimal	Catastrophic	Very unlikely	High

The fossil fuel shortage scenario combines a period of high domestic electricity consumption combined with low reserves and fuel production. Low reserves and production can have several causes, in many cases related to the above scenarios, such as weather conditions, physical attacks on infrastructure or even political reasons.

The assessment is that the scenario could have high cross-border impact, as it would turn Bulgaria from a net exporter to a net importer of electricity for the region. If our other neighbouring countries are not affected in the same way by fuel shortages, their TSOs will still be able to provide some assistance to Bulgaria.

In the event that such a scenario materialise, the probability calculation assesses the scenario as having a catastrophic impact. This is because in 2021, about 48% of the total electricity production in Bulgaria is produced from fossil fuel sources with an available capacity of over 5400 MW. However, the probability of such an event is low, as Bulgaria has a solid stock of local fossil energy resources in the East Maritsa basin. The problem is that these fossil fuels are lignite, which is heavily regulated by the EU's policy aimed at an intensive transition to a low-carbon economy and the restructuring of the electricity sector.

1.13.2 Nuclear fuel shortage

Risk profile	Impact	Probability	Cross-border impact
Minimal	Catastrophic	Unlikely	High

The nuclear fuel shortage scenario involves delaying the supply of fresh nuclear fuel in combination with high domestic electricity consumption. In this case, the supply of fresh nuclear fuel may be delayed or interrupted for various reasons. As with the fossil fuel shortage scenario described above, various causes of shortages can be found, ranging from technical problems, malicious attacks, sabotage, political problems to extreme weather conditions.

Although by the end of 2021 the share of nuclear energy in total electricity production is 35% and Bulgaria is highly dependent on it, the overall risk profile is assessed as minimal, mainly due to the statistically low probability of such an event. Given the various aspects of the current situation, it is likely that a shortage of nuclear fuel could have a catastrophic impact.

In addition, it is estimated that the shortage of nuclear fuel in Bulgaria would have a serious cross-border impact, which, as in the case of fossil fuels, would make Bulgaria a net importer of electricity in the region.

1.14 War / civil war

Risk profile	Impact	Probability	Cross-border impact
Minor	Critical	Unlikely	High

In the current conditions in the Euro-Atlantic area, there is an atmosphere of peace and the risk of the threat of a conventional attack on the territory of the EU and NATO countries is low. However, the Strategic Defence and Security Concept of NATO member-states states that the conventional threat cannot be completely ignored, as many countries and regions around the world are gaining significant modern military capabilities which could have unpredictable consequences for international stability and Euro-Atlantic security.

Although the risk of war is generally insignificant, it is still included due to the critical impact on the electricity system. In the event of military aggression, the main elements of the electricity system become the main strategic goals which are destructed. In practice, this would have a major impact on cross-border exchanges in electricity, as disabling interconnections would isolate the country from possible energy assistance from neighbouring countries.

2. ROLES AND RESPONSIBILITIES

The Minister of Energy has been designated as the competent authority for the Republic of Bulgaria in accordance with Article 3 of Regulation (EU) 2019/941, in order to facilitate the application of the Regulation together with other directly related bodies and legal entities. The role of the Minister of Energy according to the requirements of Regulation 2019/941 is:

• Article 7: to identify the most appropriate national electricity crisis scenarios and to consult the relevant stakeholders

• Articles 10, 11, 12: to establish a risk-preparedness plan in the electricity sector (the Plan), after consultation, and to publish it on the website of the Ministry of Energy.

• Article 14: To issue an early warning to the EC and other Member States that there is a possible crisis in the electricity system, its causes, planned or taken measures to prevent the crisis and the possible need of assistance; after consulting the transmission system operator, to declare an electricity crisis and to inform the other Member States and the EC, together with the reasons, planned or taken measures to mitigate its consequences and the need of assistance from other Member States.

• Article 17: To submit a crisis ex post evaluation report to the Electricity Coordination Group (ECG) and the EC within three months after the end of the electricity crisis.

ESO EAD is the certified independent transmission system operator (TSO) in the Republic of Bulgaria, which is responsible for maintaining the security of electricity supply. As a TSO, ESO EAD is also responsible for the protection, management of emergencies and restoration of the power system.

The role of ESO EAD within the Plan is to contribute to the development of regional and national electricity crisis scenarios as part of ENTSO-E according to Article 6 and to provide expertise to the relevant sections in preparing the Plan according to Article 10 of Regulation 2019/941.

To date, four licensed electricity distribution system operators (DSOs) operate on the territory of Bulgaria: CEZ Distribution Bulgaria AD, Elektrorazpredelenie Yug EAD, Elektrorazpredelenie Sever AD and Elektrorazpredelenie Zlatni Pyasatsi AD, the first three being the main ones. These companies are electricity distribution system operators and owners of the assets in the respective regions of the country. They manage the operation of the electricity distribution network in Bulgaria and work in close cooperation with ESO EAD on the aspects of the current operation, exchange of information and system defence plan. Within the framework of the System Restoration Plan, DSOs work with the National Dispatching Center (NDC) to restore the normal configuration of the power system. Additional information on these plans is presented in section 3. 1.

The role of DSOs in the framework of Regulation (EU) 2019/941 is to contribute expertise to the relevant sections in the preparation of the Plan in accordance with Article 10.

3. PROCEDURES AND MEASURES IN THE ELECTRICITY CRISIS

3.1 National procedures and measures

This section presents high-level measures and procedures applicable in the event of an electricity crisis and outlines the actions that need to be taken to maintain security of supply in the event of such a crisis. There are a number of plans, protocols, processes and procedures that define the actions of the transmission system operator and the distribution system operators in the event of a crisis. Regulation (EU) 2017/2196 establishing a network code on electricity emergency and restoration identifies the procedures and systems that guide the actions to be taken in response to an emergency. ESO EAD has an internal set of business processes that ensure that the necessary steps are taken to restore the normal operational condition of the system as soon as possible. The Rules on Power Grid Control regulate the use of the Bulgarian transmission system by all users and contain a set of actions to be taken in emergency situations.

3.1.1 System Defence Plan of Bulgaria

The System Defence Plan has been developed by the National Dispatching Center at the Electricity System Operator of Bulgaria, in accordance with the requirements of:

- Commission Regulation (EU) 2017/2196 establishing a network code on electricity emergency and restoration;
- Regulation (EU) 2017/1485 establishing a guideline on electricity transmission system operation;
- Rules on Power Grid Control;
- Policy on Emergency and Restoration, SAFA of ENTSO-E.

In developing the Defence Plan, the transmission system operator ESO EAD took into account the following elements:

- the operational security limits determined by the system operator for each transmission network element, including at least voltage limits, short-circuit current limits and permissible thermal current limits, including transitory admissible overloads;
- the behaviour and technical capabilities of consumers and producers of electricity within the synchronous zone;
- the specific needs of significant users of the transmission system of high priority and the terms and conditions for their disconnection, including the prevention of the possibility of disconnection based on voltage and frequency ranges in normal and alert state;

- the characteristics of the electricity transmission network and the adjacent electricity distribution networks.

The system defence plan contains the following provisions:

- the conditions under which the system defence plan is activated;
- the system defence plan instructions to be issued by the TSO;
- the measures subject to real-time consultation or coordination with the identified parties.

The system defence plan includes the following technical and organizational measures:

- automatic system protection schemes: under-frequency control scheme; over-frequency control scheme; actions in decrease in voltage (voltage collapse); actions in increase in voltage;
- system defence plan procedures: for frequency deviation control; for voltage deviation control; for power flow management; assistance for the active power procedure; manual demand disconnection procedure.

The measures contained in the Defence Plan are compliant with the following principles:

- their impact on system users shall be minimal;
- be cost-effective;
- only those measures that are necessary shall be activated;
- they shall not lead the power system or the interconnected transmission system into emergency state or blackout state.

3.1.1.1 Classification of the state of the power system

Regardless of the risk profile category in the electricity crisis scenarios listed in section 1.2, the actions taken by the TSO are determined by the seriousness of the situation. The level of system crisis is determined by the system alarm level. These system states range from normal to alert, emergency state, blackout state, and restoration state, with a set of defining criteria for each. In the table below, a brief description is given, characterizing each state according to the power system states classification.

State	**Criteria for establishing the state**
Normal	Normal state means a situation in which the system is within the operational security limits and all of the following conditions are met: - voltage and power flows are within the operational security limits and the configuration of the electricity transmission network meets the security criteria; - the steady state system frequency deviation is within the range of 50Hz ± 0.05 Hz or the absolute value of the steady state system frequency deviation is not larger than ± 0.2Hz and the system frequency limits established for the alert state are not fulfilled; - active and reactive power reserves are sufficient to withstand contingencies from the contingency list without violating operational security limits; - operation of the concerned TSO’s control area is and will remain within operational security limits after the activation of remedial actions following the occurrence of a contingency from the contingency list.
Alert	Alert state means the system state in which the system is within operational security limits, but a contingency from the contingency list has been detected and in case of its occurrence the available remedial actions are not sufficient to keep the normal. The system is in alert state when:

	- voltage and power flows are within the operational security limits; - the TSO's reserve capacity is reduced by more than 20 % for longer than 30 minutes and there are no means to compensate for that reduction in real-time system operation; - the absolute value of the steady state system frequency deviation is not larger than the maximum steady state frequency deviation and the absolute value of the steady state system frequency deviation has continuously exceeded 50 % of the maximum steady state frequency deviation for a time period longer than the alert state trigger time or the standard frequency range for a time period longer than time to restore frequency; - at least one contingency from the contingency list leads to a violation of the TSO’s operational security limits, even after the activation of remedial actions.
Emergency	Emergency state means the system state in which one or more operational security limits are violated. The system is in emergency state when at least one of the following conditions is fulfilled: - there is at least one violation of the operational security limits; - frequency does not meet the criteria for the normal state and for the alert state; - at least one measure of the System Defence Plan is activated; - there is a failure in the functioning of tools, means and facilities, resulting in the unavailability of those tools, means and facilities for longer than 30 minutes. The emergency state includes the splitting of the coupling into areas - operating asynchronously, significant in volume cascade accidents and loss of resilience. It is characterized by a high degree of threat to the individual control blocks (areas) and violated security criteria. This is a situation in which the control systems and the emergency automation must prevent system splitting and limit the spread of disturbances and accidents to the neighbouring parallel operating energy systems.
Blackout	Blackout state means the system state in which the operation of part or all of the transmission system is terminated. Blackout state is when at least one of the following conditions is fulfilled: - loss of more than 50 % of demand in the TSO’s control area; - total absence of voltage for at least three minutes, leading to the triggering of the Restoration plan.
Restoration	Restoration state means the system state in which the objective of all activities in the transmission system is to re-establish the system operation and maintain operational security after the blackout state or emergency state. In this state, the system operator has activated measures from the System Restoration Plan.

In classifying the system state, four types of threats are distinguished:

• Threat to the network: considers the adequacy of the baseline state or post-disturbance state against the operating criteria (transmission capacity and voltage);

• Threat to the balance between generation and consumption: considers the adequacy of the baseline state or post-disturbance state against balance maintenance;

• Threat to the communication and management infrastructure (means for ADCS), leading to deviation of the observed system parameters, outside the limits of normal system operation;

• Threat from an event that puts the parameters of the power system beyond the permissible ranges: considers the occurrence of an event that puts the parameters of the power system beyond the permissible ranges, such as exceptional weather conditions, terrorist attack, natural disaster, etc.

The power system operation depends on the interaction of the transmission system operator and DSOs. The priorities are determined by the operators (dispatchers at TDCs and NDC) of ESO EAD. DSOs need to agree on clear rules for interaction, as well as to agree on response time in different situations.

When working with operational staff in a substation, according to the regulations, staff is subordinated primarily to the operator of ESO EAD, and then to the DSOs' operators (dispatchers at the Specialised Dispatching Units (SDU). In the substations with remote control, the switching is performed from the Support point, but manipulations such as grounding, safety, etc., must be carried out by operational staff on site.

In a provision, rule or bilateral instruction, the response time of the operational staff must be agreed. The activities of the DSOs' operators are highly dependent on this time. Based on this regulation, the operator can use a certain resource in a critical situation properly, rather than waiting indefinitely for manipulations in substations, which will increase the time of loss of supply to consumers. This is also necessary in severely worsened weather conditions.

3.1.1.2 Automatic and manual system protection schemes in crisis situations

<u>Special protection system for generation island operation</u>

This is a type of special protection system set on certain thermal units of system relevance and started during significant frequency deviation in the electrical network. It is part of the under-frequency and over-frequency system protection schemes, enabling the thermal units of systemic relevance to maintain their operation and power supply for their own needs, in order to speed up the restoration of the power system after the accident. The generation island operation is an extremely rare event and is associated with the occurrence of a cascade accident, in which there is a split of the synchronous area to asynchronously operating areas or separation of an area from the interconnected system.

<u>Under-frequency special protection systems</u>

The under-frequency special protection systems and generation modes of operation include automatic load shedding, frequency control mode at the generating modules (primary regulation) and disconnection of the power storage modules, which are in user mode.

The scheme includes disconnection of demand at different frequencies, from a 'starting mandatory level' 49Hz to a 'final mandatory level' 48Hz, within an implementation range whilst respecting a minimum number of six the step and maximum size of steps of 10% of the total load in the power system.

TSO and DSOs shall install relays necessary for low frequency demand disconnection taking into account load behaviour and dispersed generation.

<u>Automatic Load-Shedding (ALS)</u>

ALS causes disconnection of demand from the electrical network (emergency shedding), in the absence of spinning reserve and system-wide deficit of active power, in order to stop further decrease of frequency and restore the established system operating mode at an acceptable level above 49Hz. ALS is carried out by voltage devices with frequency patterns and logic, installed in the transformer substations 110/MV, which react to disconnection of MV terminals. ALS should block Automatic Load Transfer (ALT) and autoreclosures. The total volume of electrical demand that can be disconnected from ALS should not be less than 45% of the total system load at any given time. Each ALS device must be able to perform the functions ALS-I, ALS-II, accelerated ALS and be able to disconnect consecutively four groups of users to a given MV section, always starting from the first to the fourth group.

Under-frequency control scheme

49.8 Hz	Frequency sensitive mode - allocation of the reserve for primary regulation
49.8 – 49.2 Hz	Automatic or operative disconnection of pumps in PSHPP; Automatic or operational mobilization of the available spinning reserve in TPPs and HPPs; Automatic or operative commissioning of hydro units in HPPs
49.0 Hz	Transition of HPP turbine regulators to speed regulation (JFC)
49.0 – 48.0 Hz	Action of ALS
48.8 Hz, 0.2s	Transition of NPP turbine regulators to speed regulation
48.7 Hz, 0.5s	Operation of frequency interconnection automation between Bulgaria and Serbia, Republic of North Macedonia, Greece and Turkey
48.0 Hz, 0.2s	Separation of HPPs (gas-steam power plants) from the transmission network
47.9 Hz, 0.3s	Operation of frequency interconnection automation between Bulgaria and Romania
47.5 Hz	Generation island operation of system TPPs and region operation 1st degree, 0.5s - large area II-nd degree, 1.0s. - medium region III-rd degree, 1.5s. - small region IV-th degree, 2.0s. - disconnection of TPPs from the electricity transmission network and supply of own needs
47.5 Hz, 0.2s	Separation of park modules and asynchronous modules from the transmission network
47.5 Hz, 2s	Separation of synchronous modules from the transmission network
46.5 Hz, 6s	Disconnection of HPPs

The groups of terminals that are allocated for disconnection at activation of ALS are determined by the DSO's operators and agreed with the operators of ESO EAD. It is carried out in order to preserve the power supply to consumers for whom the interruption of the power supply would lead to critical impacts on human health and life.

Automation and actions at increased frequency

The scheme for automatic over-frequency control shall lead to an automatic decrease of the total active power injected in each LFC area.

The transmission operator determines the parameters and the schemes for automatic over-frequency control, including the frequency thresholds for its activation and the degree of reduction of active power injection, taking into account the frequency sensitive mode of generating modules (primary control).

If the limited frequency sensitive mode — over-frequency is not sufficient, the system operator shall set up a step-wise linear disconnection of the electricity generation in its LFC area.

Over-frequency control scheme

50.3 Hz	Disconnection of renewable energy from the transmission network after 0.2 s

50.3 Hz	Automatic fast load-shedding of HPPs to the minimum allowable power for continuous operation
50.3 Hz	Disconnection of co-generation units from the transmission network after 2.0 s
50.4 Hz	Automatic fast load-shedding of TPPs to the technological minimum
50.5 Hz	Transition of NPP turbine regulators to speed regulation after 0.2 s.,
51.0 Hz	Transition of HPP turbine regulators to speed regulation (aggregates joint frequency control)
52.0 Hz	Automatic frequency disconnection of TPPs from the electricity transmission network and supply of own needs, after 2.0 s
52.5 Hz	Disconnection of HPPs from frequency protection after 20… 35 s (the time setting is determined during the test for sudden nominal load-shedding).

Undervoltage automation and actions

The automatic scheme against voltage collapse includes the following actions:

• operation of the automatic voltage regulators of the generating modules;

• automatic connection of capacitor batteries to the transmission network;

• actions for disconnection of shunt reactors to the transmission network;

• undervoltage automatic load-shedding;

• • blocking of the on-load switches of the transformers at decreased voltage.

Undervoltage automatic load-shedding

Based on its research, NDC identifies the areas of the electricity network where there is a risk of accidental voltage drop, loss of stability and risk of voltage collapse. In these areas, load-shedding automation is introduced when the voltage of the busbars of 110/MV substations is decreased, which acts to disconnection of the terminals included in the ALS.

Automatic voltage regulators in synchronous generating modules

Automatic voltage regulators (AVR)

AVRs are directly related to the automatic voltage regulation in the electric network and the stability of synchronous generators. The mass commissioning of static excitation systems with high-speed digital excitation regulators has significantly increased the possibilities for maintaining the resistance of synchronous generators to disturbances and oscillations in the power system.

Power System Stabilizers (PSS)

The main function of the power system stabilizer is to balance the rotor oscillations of the generators in the power plants, caused by a sudden change in the operating mode or power swing of the active power in the power system. This expands the operational stability range in the system (increases the possibility of power transfer). PSS is switched on automatically after the respective generator enters in parallel operation with the power system. Unauthorized removal by the plant’s staff of PSS is considered non-compliance with an operational order of the system operator.

Overvoltage automation and actions

The over-voltage automation includes the following actions:

• operation of the automatic voltage regulators of the generating modules;

• actions for disconnection of capacitors to the transmission network;

• automatic connection of shunt reactors to the transmission network;

• automatic disconnection of 400kV power lines that are idle state.

Overvoltage special protection scheme (Overvoltage SPS) - 400kV

In order to protect the electrical equipment in the electricity transmission network from unacceptably high voltages, the 400 kV power lines are equipped with Overvoltage SPS. The settings of the Overvoltage SPS must ensure the normal operation of the most voltage change sensitive element in the node. Usually, the insulation parameters of power transformers determine the lowest limiting conditions in overvoltage cases.

Frequency deviation management procedure

The procedure for the management of frequency deviations contains a set of measures to manage a frequency deviation outside the frequency limits defined for the alert state. The frequency deviation management procedure must meet at least the following requirements:

• the decrease of generation shall be smaller than the decrease of load during under-frequency events;

• the decrease of generation shall be greater than the decrease of load during over-frequency events.

Prior to the activation of the automatic low frequency demand disconnection scheme and provided that the rate of change of frequency allows it, the system operator, directly or indirectly through the distribution networks, activates demand response from the relevant service providers and:

• switches energy storage units acting as load to generation mode at an active power set-point;

• when the energy storage unit is not capable of switching fast enough to stabilise frequency, manually disconnects the energy storage unit.

Voltage deviation management procedure

When controlling the voltage deviation, the system operator uses the following (manual) remedial actions:

• switches the deviations of the windings (tap changers) of system transformers and autotransformers;

• switches capacitor and shunt reactors;

• switches power-electronics-based devices used for voltage and reactive power control;

• blocks the automatic voltage regulation of the transformers;

• changes the voltage or reactive power settings of the synchronous power generating modules connected to the transmission network;

• changes the voltage or reactive power settings of the converters of the asynchronous (park) power generating modules connected to the transmission network.

Active power flow deviation management procedure

Active power flows in the power system are managed by the transmission system operator in order to ensure that the system is operated within the thermal limits of the transmission facilities. When controlling power flows, the system operator uses the following (manual) remedial actions:

• modifies the duration of a planned outage or return to service of transmission network elements to achieve operational availability;

• angle shifting of autotransformers;

• changes the topology of the transmission network;

• recalculates the day ahead and intraday cross zonal capacities, etc.

Assistance for active power procedure

In case of absence of control area adequacy in the day-ahead or intraday timeframe, and prior to any potential suspension of market activities, the system operator is entitled to request assistance for active power from:

• any balancing service provider which, upon the operator's request, shall change its availability status to make available all its active power, provided it was not already activated through the balancing market, and conforming to its technical constraints;

• any SGU connected in its LFC area, which does not already provide a balancing service to the system operator, and which, upon request, shall make available all its active power, conforming to its technical constraints;

• other TSOs that are in the normal or alert state.

Manual demand disconnection procedure

The system operator may establish an amount of the netted demand to be manually disconnected, directly or indirectly through the distribution networks, when necessary to prevent the propagation or worsening of an emergency state. Where demand is to be directly disconnected, the system operator informs the relevant distribution system operators without delay.

The system operator activates the manual disconnection (dispatching order) of the net load in order to:

• resolve overloads or under voltage situations;

• resolve situations in which assistance for active power has been requested but is not sufficient to maintain adequacy in day-ahead and intraday timeframes, leading to a risk of frequency deterioration in the synchronous area.

The system operator notifies DSOs of the amount of netted demand to be disconnected on their distribution networks. Each DSO disconnects the notified amount of netted demand, without undue delay.

Within 30 days of the incident, the system operator shall prepare a report containing a detailed explanation of the rationale, implementation and impact of this action and submit it to EWRC in accordance with Article 37 of Directive 2009/72/EC.

According to Chapter II, Section 3 of Ordinance No. 3 on the design of electrical installations and power lines, in terms of security of electricity supply, electricity consumers in Bulgaria are divided into four categories - null, first, second and third.

Null category includes consumers for which the interruption of electricity supply can endanger the people's life and health, cause a threat to state security, significant material damage, disruption of complex technological processes, disruption of particularly important economic facilities, communication systems and television. Null category users include:

1. special installations and life support systems in hospitals;

2. signalling and security systems;

3. systems for informing the population in case of disasters;

4. places with use of emergency and evacuation lighting, etc.

The first category includes consumers for which the interruption of electricity supply causes disruption of important infrastructure of settlements, disruption of complex technological processes, mass scrapping of production with significant losses.

The second category includes consumers for which the interruption of electricity supply causes the cessation of mass production, downtime of workers, equipment and industrial transport, as well as disruption of the normal living conditions of a large number of people. The second category of consumers also includes residential buildings with high construction, administrative and public buildings, etc.

The third category includes all other users who do not fall into the categories - null, first and second.

Null-category consumers are supplied with electricity from two independent mutually redundant power sources and from a third autonomous independent source. The permissible interruption of the power supply of a null category user is only for the time necessary for its automatic recovery from the backup source. In the case of life support systems and special cases that prevent power outages and for the time of automatic recovery, the continuity of power supply is ensured by the autonomous independent source.

The first category consumers are supplied by two independent mutually redundant sources. The permissible interruption of the power supply to a first category user is only for the time of the automatic switching from one source to another.

Second category consumers are supplied by two independent mutually redundant sources. The permissible interruption of the power supply to a second category user is for the time of the manual switching from one source to the other, performed by operative or operative-repair personnel.

Third category consumers are supplied with electricity from a single power source, provided that the interruption of the power supply necessary for the repair or replacement of a damaged element of the power supply system does not exceed 24 hours.

At the request of the clients, EDCs can assist in the construction of facilities for another category, where the responsibility for compliance with the redundancy lies with the client.

In the presence of shortage or overproduction of electricity according to the Rules on Power Grid Control (Issued by the Chairman of the State Energy and Water Regulation Commission (now EWRC), promulgated, SG, iss. 6 of 21.01.2014, amended, issue 100 of 15.12.2017, in force since 15.12.2017) and Ordinance No. 10 of 9.06.2004 on the procedure for introducing a restrictive regime, temporary interruption or curtailment of electricity production or supply, thermal energy and natural gas (Issued by the Minister of Energy and Energy Resources, promulgated, SG, iss. 63 of 20.07.2004, effective 20.07.2004, amended, issue 42 of 9.06.2015, in force since 9.06.2015) ("Ordinance 10") measures are taken to limit consumption or production according to pre-prepared programs agreed with ESO EAD. The implementation and the manner in which they will be carried out are determined operatively by the dispatching units of ESO EAD.

EDCs strictly follow the instructions of ESO EAD and report in case of discrepancies or non-compliance by energy companies or producers.

Dedicated aggregates and systems for uninterruptible power supply, batteries, etc.can be used in addition to the power plants as a third independent source for electricity supply to consumers of null category and as a second independent source for consumers of first category.

3.1.2 System Restoration Plan of Bulgaria after severe accidents

The power system restoration plan is a procedure used in case of partial or complete separation of the power system. As a result of the serious nature of this event, all users of the electricity transmission network of system relevance are obliged to maintain a high level of awareness and training on the issues of system restoration. The ultimate goal is to ensure that customers are reconnected safely and as quickly as possible. The Restoration Plan defines:

- the general principles for the power system restoration after its complete separation;
- the distribution of the functions and actions of the operational staff of the transmission system operator, power plants of system relevance and the distribution network operators;
- the main restoration scenarios (description of corridors) that can be combined and applied to specific emergencies;
- the priorities and the sequence in the power system restoration;
- the main starting power sources in the power system restoration;
- actions of operational personnel in the absence of telecommunications.

The restoration of the power system after its complete or partial separation goes through the following possibilities and stages:

I. Restoration through assistance from neighbouring power systems - establishing an energy corridor from a neighbouring power system ("top-down" principle) is a priority way to restore the power system of Bulgaria. Where assistance from neighbouring power systems can be chosen, it starts with the system, which is currently better connected to the Continental European network. The plan envisions energy corridors from Romania, Serbia, Republic of North Macedonia, Greece and Turkey.

II. **Restoration through the use of local starting sources (HPPs with the possibility of "black start")** - Establishing an energy corridor from the start-up HPPs ("bottom-up" principle) is applied when no neighbouring power system is able to provide electricity assistance to Bulgaria.

III. **Establishing energy corridors to TPPs and NPP** - **an energy corridor** is a set of facilities (substations and power lines) that provide power to the own needs of priority thermal power plants from start-up sources. Establishing an energy corridor from the start-up HPP to Kozloduy NPP is applied only if there is a malfunction in the supply of safety systems from the diesel generators of Unit 5 or Unit 6. Then, the establishment of an energy corridor to a priority TPP is postponed until later, when the power supply activities at Kozloduy NPP are secured.

IV. **Expansion of the corridors and ensuring power balance** - in the process of expanding the energy corridor, new power plants are successively launched, and loads are introduced in the substations, continuously ensuring power balance. Corridors and islands are widened until certain substations equipped with synchronization equipment are reached.

V. **Connection of self-operating areas and energy corridors in a common power system** - the synchronization between two regions/corridors is performed in substations that are equipped with synchronizing equipment. If it is possible to synchronize two self-operating islands or an island with part of the power system on several power lines in one site, first is the power line with the highest transmission capacity (strongest connection). After synchronization and merging of two self-operating islands, only one power plant should remain in "frequency control" mode. The other power plant must be switched to "active power control" mode.

VI. **Restoration of the parallel operation of the Bulgarian power system with the neighbouring power systems and the planned cross-border exchanges** - the interconnection of the entire electricity transmission network is restored, after which transition is made to parallel operation of the Bulgarian power system with the neighbouring electricity systems that are in normal state. After the power system of Bulgaria starts parallel operation with the Continental Europe power system, the planned cross-border exchanges are restored.

VII. Restoration of power supply to all customers

3.1.3 Mechanisms for informing the public in electricity crisis

Different types of communication are used to inform stakeholders, including producers, distribution system operators, internal staff, the energy regulator and the market operator, that the power system is in an unusual state. Each user of the system is responsible for their internal procedures upon receipt of such a warning. The Minister of Energy is responsible for communication with the EC and other Member States regarding early warnings and alerts in accordance with the requirements of Regulation 2019/941. Market participants are informed through market couplings.

The table below summarizes the communication methods used to communicate with key stakeholders.

At all times, during operation and in the operational planning phase, each system operator shall communicate to the other system operators the state of its own power system, based on a security assessment, taking into account internal or regionally agreed remedial actions. This information must be analysed in case of any change in the power system state.

In case of change in power system state from Normal to Alert, Emergency or Blackout, messages are sent in accordance with the procedures approved by RG CE (Regional Group Continental Europe) and described in the Crisis Communication Tool and ENTSO-E Awareness System. Subsequently it is specified: the type of threat and the nature of the criterion violated. Other system operators need to assess the impact on their own control blocks/areas. Under certain conditions (eg. frequency deviation), pre-prepared messages can be sent automatically.

Stakeholder	**Communication methods used by ESO EAD**
Generators	E-mail Telephone Fax SCADA signal Message on the market platform
EDC	E-mail SMS SCADA signal Telephone Fax
Regulator and government bodies	E-mail Telephone Fax
Power exchange operator	E-mail Telephone Fax Market message
Other TSOs	Telephone Fax ENTSO-E Awareness System
Market participants	Communication on the market platforms of TSO and the power exchange operator E-mail
Public and media	Through a message on the website of ESO and the press center Message on social networks

3.1.4 Procedures and information flows in electricity crisis

SCADA systems are a set of software and hardware that enable local or remote control of the parameters of automated technological processes in a number of industries.

The main function of these solutions is the software of automation systems in process industries. Modern SCADA platforms also allow complex monitoring, data collection and processing in real time, as well as recording events in the form of logs.

The basic hierarchical structure of SCADA systems includes four separate levels with clearly distributed functions:

- field equipment;
- programmable logic controllers (PLC) and/or Remote Terminal Units (RTUs);
- communication network;
- SCADA software.

Real-time information in the process of electricity crises is carried out mainly through the data management and collection system (SCADA/EMS) for the sites of the transmission network and covers:

• flows of active and reactive power in the transmission network;

• voltages and frequency of busbar systems and power lines;

• position of the tap changers of the system autotransformers (entered manually or automatically);

• active and reactive capacities of production units;

• capacities of capacitors - shunt reactors and capacitors;

• state of the switching devices;

• automatic operation of relay protections on main elements of the transmission network;

• malfunctions of the main means of communication;

• main parameters of the mode of operation of border substations of neighbouring power systems. The means of communication between the individual dispatching centers and between the dispatching centers and the major sites of the transmission network are backed up. SCADA/EMS system is backed up with a completely independent system in terms of interconnectors and border substations.

For the interconnection 400kV power lines there is information from the main and backup telemechanical system (basic position of the circuit breakers on the power line and measurements of active P and reactive Q power, voltage U and frequency f).

NDC and RDCs are equipped with diesel power generators, which provide the ability to perform basic functions for a long period of time, not less than 24 hours. NDC is able to continue operation in the case of an inoperable main dispatching center through a backup dispatching center.

Substations of system relevance must be equipped with diesel generators, which provide the ability to perform operational switching and the operation of protective, telemechanical and communication devices for a long period of time, not less than 12 hours. A list of substations with instructions for the minimum required systems that must remain supplied for the specified period is given in Annex 7.5.

The transmission system operator, the distribution system operators and the operational staff of the users participating in the Restoration plan exchange telephone numbers and names of the officials responsible for the organization and operation of information points operating in the event of system accidents.

The actions of the operational personnel in the electric power sites in case of system accidents, partial or complete separation of the power system are described in the System Restoration Plan of Bulgaria in section 3.

The practice of EDCs is similar. The dispatching units are backed-up for the purpose of uninterrupted power supply. The channels for communication are backed-up both within the EDC and to ESO EAD, ME and other structures in the energy sector.

3.1.5 Preventive and preparatory measures

General measures have been introduced to protect and prepare the power system for future changes. These measures are triggered by both European and national legislation.

Every year, ESO EAD prepares a Network Development Plan which sets out the intentions for the development of the electricity transmission network of Bulgaria and interconnections for a period of ten years. It presents the projects that ESO EAD considers necessary to strengthen the electricity transmission infrastructure and which will help achieving the strategic goals set by national and EU policies, including projects of common interest (PCI). This plan is prepared after intensive correspondence with current and future investors, taking into account the preliminary contracts for the construction of new generating capacity. In addition, the Plan contains projected energy balances and power balances for expected extreme loads, which serves as a simplified and deterministic assessment of long-term adequacy. This helps to identify potential adequacy gaps that could jeopardize security of supply and allows future transmission system users to gain a better idea of the possibilities for connecting new sites.

EDCs implement measures related to preventive activities to increase the reliability of the elements of the electricity distribution network, as well as modernization of the network itself.

Periodic inspections of the facilities are carried out. Their readiness for operation is assessed. Measures are taken to improve their characteristics and, where necessary, they are replaced with new ones. After analysis of the network, activities related to the replacement of the network or elements of it are carried out, as well as the application of new innovative technologies and facilities.

3.1.5.1 Cybersecurity

Tackling cybersecurity threats is a growing concern in the energy sector, as analysis shows that the number of reported attacks on utility providers worldwide has increased in recent years. Regulators and legislators are trying to address the threat by tightening instructions to operators and introducing legislation that requires a minimum set of cybersecurity control measures. Within the EU, the Network and Information Systems Regulation (NIS-D), which was successfully implemented in Bulgaria in 2018, seeks to address this issue by identifying essential service operators (ESPs) and recommends a minimum standard for cybersecurity control, as well as mandatory requirements for cyber incident reporting. The State Electronic Government Agency has been appointed as a competent body in the Republic of Bulgaria. NIS-D obliges all ESPs to achieve and maintain a minimum level of cybersecurity maturity in order to reduce cyber risks and threats in the performance of their critical activities. According to NIS-D, the relevant competent authority measures the compliance of ESPs with the requirements of the regulation by assessing the level of compliance with security controls.

As a transmission system operator, ESO EAD is defined as an ESP within the meaning of Regulation (EU) 2016/1148 and is subject to more formal management and reporting measures on cybersecurity controls for critical systems and processes. The measures focus on logical access control for the systems and applications used by operators in the control room. Logical access control is a key component in protecting computer environments and can be complemented by physical access control and residual risk management monitoring. Standards for logical access control in a control room environment must be designed in such a way that they do not introduce undue complexity that may impede or delay operators' access to critical emergency systems, and should be complemented by a stable physical access control.

Regulation (EU) 2019/943 on the internal market in electricity provides for the development of a new EU Cybersecurity Network Code. It will provide a common set of rules and minimum requirements for cybersecurity throughout the electricity sector, including across borders. The Code is currently being developed, main drivers being ACER (the Agency for Cooperation of the Energy Regulators), ENTSO-E and the Organization of European Electricity Distribution System Operators (E.DSO).

3.1.5.2 Physical attack

Access to all power system control rooms and the adjacent critical infrastructure is strictly controlled by means of sophisticated access control systems. The security of the buildings and the monitoring of the sites is done by security guards and security system, in order to guarantee only legitimate entry into them.

3.1.5.3 Insider threat

As a result of the correct social policy and selection of the staff in the energy companies with public functions, a conscientious attitude towards the official duties and striving for protection of the entrusted property is formed. In addition, applicants for employment in NDC of ESO EAD are subject to increased scrutiny by the State Agency for National Security prior to their appointment, as NDC is on the list of sites of strategic relevance for the electricity sector. The state of the most critical elements for preventing accidents and incidents is monitored. For this reason, it should be noted that the risks of sabotage, vandalism and theft committed by company employees are minimized.

It should be noted that currently ESO EAD lacks data and documents describing forms of malicious act by an employee or subcontractor.

Trainings for work on processes and instructions are conducted in EDCs. Quality control systems have been introduced, and in case of non-compliance with any of the processes, an analysis is made and measures are taken to limit the identified negative phenomena. Thus, the possibility of escalation of the problems with an internal cause is not allowed as a preventive measure.

Careful selection of the partnering companies is made. Continuous supervision of the work is performed, as well as inspection of the performed activities.

Risks of accidental error are limited through the "4 eyes" principle.

3.1.5.4 Natural disaster and extreme weather conditions

Extreme weather conditions, storms

Transmission and distribution networks are designed for service continuity and safety within economic constraints. The design and construction are in accordance with Ordinance No. 3 on the design of electrical installations and power lines, including requirements related to meteorological conditions, such as wind and static ice load. The distribution network is generally exposed to less wind loads than the transmission network, as it is closer to the ground (usually less than 10 m).

Every year, NDC prepares a report on the operational mode of the Bulgarian power system during the forthcoming autumn-winter period. The report focuses on the analysis of the flow distribution by examining the normal and boundary modes of operation of the transmission electricity network of Bulgaria during the winter period, in order to determine:

• the loading of the elements of the electrical network;

• expected voltage levels;

• the fulfilment of the security criterion N-1 for the transmission electric network;

• the conditions for optimal operation of the electricity network with minimal losses of electricity from transmission and transformation;

• the possibilities for voltage regulation within the admissible limits and the necessary technical means;

• the transmission capacity of the electricity network in the exchange of electricity with neighbouring power systems.

The developed calculation models are summarized perspective calculation models of the power system of the countries of Southeast Europe for the absolute winter maximum mode, average working day mode and minimum mode for weekend. The absolute maximum mode is the starting point for determining the expected maximum load of the electrical network in normal and repair schemes. The average working day mode is necessary to determine the economic operation of the power system during the planned period, in terms of power losses in the grid, and the minimum regime is boundary to calculate the maximum voltage in the grid for the planned period and check the adequacy of voltage control. After taking into account all the characteristics of the regions and analysing the results of the flow distribution task, the report gives conclusions and recommendations on the general state of the electricity system, expected critical elements of the network, the need for additional voltage regulation and preventive switching, in order to ensure the normal mode of operation of the power system during the upcoming winter period.

The same tools are used in the preparation of EDCs for autumn-winter operation of the facilities. For the Black Sea region, this is done in the spring before the active summer season.

Wildfire

The risks of forest fires are reduced by maintaining the easement areas through cutting down wood near the overhead lines of the transmission network, the so-called clearing. This ensures minimal distances between vegetation and electrical infrastructure. The minimum insulation distances for open distribution systems and overhead lines are subject to regulation and are defined in **Ordinance No. 3** on the design of electrical installations and power lines.

Earthquakes

The measures for prevention and reduction of the risk of earthquake according to the National Disaster Protection Plan are:

• research, analysis and assessment of the seismic risk for the territory of the country;

• updating seismic zoning and conducting microseismic zoning where necessary;

• categorization of the territory of the country in terms of seismic risk;

• Completion of the technical certification of the constructions in time, emphasizing the degree of seismic protection;

• geoprotection and shore protection measures;

• exercising strict control for strict compliance with the relevant regulations in the spatial planning, investment design and implementation and operation of constructions;

• compliance with the provisions for design and construction in seismic areas - Ordinance No. RD-02-20-19 of 29.12.2011 on the design of building structures of constructions through the application of the European system for design of building structures (Promulgated, SG, issue 2 of 2012) and Ordinance No. RD-02-20-2 of 27.01.2012 on the design of buildings and facilities in earthquake areas of the Minister of Regional Development and Public Works (Promulgated, SG, iss. 13 of 2012);

• strengthening of depreciated secured and unsecured buildings and facilities;

• development of scenarios for the consequences of strong earthquakes for large urban areas, in order to identify the most vulnerable places and additional measures, if necessary;

• training course for proper behaviour before, during and after major earthquakes in all levels of education;

• training and practical exercise of the central and territorial bodies of the executive power, the response forces and the population;

• development and implementation of effective early warning systems;

• international exchange of information, data and scientific and practical cooperation with neighbouring countries and European centers;

• creation of a fund (with accumulation) to cover the consequences of earthquakes.

Pandemic

In the event of a pandemic, energy companies take action to limit staff contact by using remote forms of communication and mandatory use of personal protective equipment.

Conducting events to inform staff about the dangers. Taking preventive measures to limit the damage to the personnel of the EDCs.

All employees are provided with personal protective equipment, securing healthy conditions for the work process. Disinfection of workplaces is carried out. The measures are periodically updated, depending on the external information received from the anti-epidemiological headquarters.

Periodic conducting tests to establish the real health state of the staff. Identifying persons with increased risk of infection and determining measures to protect their health. In cases of signs of illness, non-admission of employees to work places - quarantine. The distribution by work areas, without the possibility of direct contact, both with external persons and within the company.

As an employer, contribution to the successful course of the vaccination process.

In particularly severe situations, the work process is carried out in isolated premises (for the operational staff where on 24 h mode), without leaving the workplace, until the termination of anti-epidemic measures.

Heavy rainfall and flooding

System substations and dispatching centers of ESO EAD are located in low-risk areas and are not at risk of flooding. In certain places in the country there may be a forced interruption of the power supply with a limited range or rotational preventive outages in order to prevent a major accident until damage is repaired or water is drained.

EDCs carefully monitor the ME forecasts for floods and high waters. If necessary, preventive disconnection of the voltage in the endangered sites is performed. In particularly difficult situations, where possible, preventive relocation of equipment to a safe place is envisaged.

3.1.5.5 Technical failure

Failure of critical ICT systems

The growing dependence on the use of information and communication technology poses a moderate risk in the event of failure of one or more elements of it.

ESO EAD implements an investment policy aimed at permanent reconstruction and rehabilitation, including of hardware, software, communication channels and control and management systems.

The means of communication between the individual dispatching centers and between the dispatching centers and the major sites of the transmission network are backed up. SCADA/EMS system is backed up with a completely independent system in terms of interconnectors and border substations. In case of physical damage in NDC, ESO EAD may transfer the management to a separate back-up operational center in case of emergency.

Regardless of the measures taken to provide the necessary telecommunications, it is possible that some sites will be temporarily unable to communicate with the relevant dispatcher. This requires, in such a situation, to carry out the appropriate manipulations which will facilitate and speed up the actions of operational staff after the restoration of telecommunications.

Given the diversity of local conditions, here and in the OPERATIONAL ORGANIZATION LIST are the basic guidelines for the actions of local staff in the absence of telecommunications The local instructions shall specify the specific actions that the operational staff shall carry out independently in the event of loss of telecommunications, as well as the operations which may be carried out independently.

The criteria for occurrence of a system accident in the absence of telecommunications between the site and the dispatcher from RDC/ NDC are:

- voltage loss on all busbar systems and simultaneously triggering of at least one stage of automatic load shedding (ALS) or generation island operation
- 20 minutes after voltage loss on all busbar systems.

Voltage loss of all busbar systems without ALS or generation island operation is not usually a criterion for a system failure. Such an effect also results from local damage such as: short circuit of busbars, short circuit of terminal with breaker failure, etc.

In case of complete loss of voltage on all busbar systems and lack of telecommunications with the dispatchers of the respective RDC, detailed descriptions of the actions to be taken by the operational staff of the respective energy sites are given.

Human error

The energy companies engaged in the production and transmission of electricity employ highly qualified personnel who are subject to periodic instruction and control of knowledge. Apart from that, the companies take constant care of the staff training, conduct periodic and extraordinary briefings related to the safe operation of the facilities. An appropriate social policy is implemented, which motivates employees to strictly follow the rules and requirements of labour discipline. This is crucial for minimizing the risk of human error in the system.

3.1.5.6 Fuel shortage

Article 8 and Article 9 of Ordinance No. 11 of 10.06.2004 for fuel reserves in case of complete interruption of the supply of fuels for TPPS on solid, liquid and gaseous fuels determine the required quantities of reserves of primary and secondary fuel, corresponding to of the forecast and/or agreed mode of operation of the power plant for a different number of days - ranging from 5 to 30 days.

Art. 10 states that an electricity producer operating a nuclear power plant shall collect and maintain reserves of fresh nuclear fuel not less than the fresh nuclear fuel required to refuel one power unit of each type of installed capacity on one site.

However, if the fuel shortage is permanent and the primary and secondary fuel stocks of conventional power plants are depleted, this would cause a huge energy crisis by excluding unprotected consumers from the grid for long periods of time.

3.1.5.7 Political

Providing countries with sufficient quantities and quality, as well as affordable, energy resources is a major task in world politics and the policy of all EU member states. Bulgaria pursues a policy of active participation in the implementation of EU strategic initiatives. It participates in the development of an integrated and competitive energy market, as well as in building the necessary infrastructure and diversifying energy supplies in order to reduce its energy dependence.

War / civil war

As the share of global energy consumption increases, energy supplies are increasingly at risk of disruption in order to exert political pressure or cause economic losses to affected countries. For this reason, NATO has identified ensuring the community’s energy security as a key task in military planning. The analysis of the current security environment performed by international military analysts shows that the risk of war remains relatively low for now, but cannot be excluded, and this risk may appear suddenly and escalate in a very short time.

The impact of a possible military invasion on the physical integrity and modes of operation of the power system is almost always detrimental, which would lead to forced interruption of electricity supply to end users in the long run.

When a crisis is declared, a Crisis Staff is convened at EDCs. Measures are taken to assess the state, assess the available resources and redistribute them if necessary.

In case of escalation of the emergency, the crisis staff takes over the management of the affected territories. Priority is given to measures related to limiting the harmful impact and restoring the normal operation of the facilities in the electricity distribution network. Restoring customer power supply in the fastest way possible.

Setting priorities when restoring the power supply to the facilities:

- Substations and junction stations
- MV terminals
- of transformer station groups with a large number of clients
- all other facilities including LV network
- in case of impossibility to supply the customers with a generator, as well as ensuring its current operation during operation.

3.1.6 Regional and bilateral procedures and measures

Bilateral operational agreements

Based on the specific requirements and recommendations described in the ENTSO-E Synchronous Zone Framework Agreement (SAFA) concerning Continental Europe Regional Group (RG CE), ESO EAD has concluded bilateral agreements for transmission network operation (Operational Agreements) with the TSOs of all neighbouring countries of Bulgaria: TRANSELECTRICA (Romania), ADMIE/IPTO (Greece), EMS (Serbia), MEPSO (Republic of North Macedonia) and TEIAS (Turkey). The bilateral operational agreement regulates the technical issues and details at parallel operation of the two systems to the Continental Europe synchronous area and covers the following topics:

1. Management of the frequency and load of the power system and the related reserves - the boundaries of the two control areas are determined;
2. Preparation of electricity exchange schedules, settlement and allocation of cross-border transmission capacity;
3. Operational security - includes information and general principles on the list of external network elements of common interest in emergencies, list of external observable network elements, operational constraints and parameters, single-line schemes of border substations, criterion N-1 in network calculations, settings of synchronization equipment and relay protections of interconnection power lines, voltage and reactive power regulation, short-circuit currents, calculations on static and dynamic stability and transmission network development plans;
4. Coordinated operational planning - includes information and general principles on the list of mutually influencing network elements in switching, coordination of planned downtime, manipulations and permits for work and calculation and coordination of interconnection capacity;
5. Power system operation in emergencies and restoration - includes information and general principles for determining the operational state of the power system according to the ENTSO-E Awareness System classification, decreased frequency action plan, power system restoration, high disturbance frequency management and resynchronization;
6. Communications - includes information and general principles on communication infrastructure, real-time data exchange, official language and time zone, means of oral and written correspondence, authorized staff;
7. Operational training - general information about the forums and programs for mutual training of the operational staff of both countries
8. Commercial metering devices and reporting - general information and principles

Emergency energy supply contracts

As of the beginning of January 2021, ESO EAD is in the process of signing a contract with IPTO for mutual emergency supply of energy to secure system services between the electricity systems of Greece and Bulgaria.

The purpose of such an agreement is to establish the conditions and rules under which the parties will provide mutual energy assistance in emergencies, using the available reserves in real time, without jeopardizing the security of the power system entrusted to them.

The subject of the contract is the emergency supply of energy from the electricity system of the Provider to the electricity system of the Recipient through a high voltage interconnection in order to cover the needs of the Recipient. This emergency supply of energy is reciprocal between IPTO and ESO EAD, and both parties can be Suppliers or Recipients of emergency energy. Emergency energy is supplied by each of the Providers in case of damage to major generating or transmission devices, which adversely affects the security of the electricity system of the Recipient. Emergency power supply in parallel operation is considered to be an appropriate and timely change of the CAS/SAS (Control Area Schedule/Scheduling Area Schedule) files of both parties. The supply of energy in emergency situations depends on the technical capabilities, available reserves and the remaining available cross-border capacity and must not affect the cross-border capacity offered on the market or the capacity already nominated.

The price at which the payment for the delivered emergency energy is envisaged is calculated on the basis of the clearing price on the national day ahead market of the supplier for the period under consideration plus a premium.

4. Crisis coordinator

The Minister of Energy, as the competent body, is responsible for ensuring the security of the electricity system. He monitors and analyses the situation regarding the security of generation, transmission and distribution of electricity, coordinates activities in case of crisis, announces the separate crisis levels in case of emergency within the meaning of Regulation 2019/941, introduces curtailments on the consumption of electricity for certain periods of time on the territory of the Republic of Bulgaria or part of it in case of emergency within the meaning of Regulation 2019/941, is responsible for communication with the European Commission and provides information on the application of both market and non-market measures to verify the correctness of the declared state of emergency, through its representative participates in the sessions of the Coordination Group at the Directorate General for Energy of the European Commission and ensures the exchange of information between the European Commission and the Ministry of Energy.

In order to deal with crisis situations, the plan defines the responsibilities and obligations of crisis management bodies and their members, to ensure their effective and timely response in case of emergencies that could disrupt the smooth supply.

4.1. The main body in the Ministry of Energy for the management of the department in the event of a crisis is the Departmental Staff. It is a non-staff body, which is established by order of the Minister of Energy, pursuant to Article 63 para. 2 of the Disaster Protection Act. The Departmental Staff acts as a crisis management group. The Departmental Staff assists the managers of the Ministry of Energy in carrying out disaster protection activities, management of crisis and emergency of non-military nature caused by natural disasters, fires, catastrophes, accidents, criminal activity, terrorism and other circumstances of social, economic and political nature in which the normal functioning of the energy system is disrupted, instability in the political and social environment is caused, life, health, property of citizens, cultural and material values, environment and in general the national security of the country are endangered. The Minister of Energy, who is also a competent body, exercises control over the activities of the Departmental Staff.

4.2. The structure of the Departmental Staff is determined by the order of the Minister of Energy, appointing heads from the Ministry of Energy who have the necessary expertise and experience in crisis management and are familiar with the regulations governing protection in disasters and crises of various kinds.

4.3. Departmental Staff carries out the following basic tasks:

- establishes constant communication with the National Disaster Protection Staff (NDPS) and the crisis staff of the energy companies from the energy sector, located in the disaster zone or affected by the crisis/emergency situation;
- through the duty officers in the Ministry of Energy, receives up-to-date information on the situation in the affected areas. Works to achieve maximum efficiency in the implementation of measures to protect the population and infrastructure and prevent interruptions in electricity supply;
- analyses the information received from the companies and the NDPS, assesses the degree of destruction and the harmful consequences of a disaster or crisis/emergency situation in the energy system and determines measures for immediate implementation;
- assesses the situation, composition and state of the response forces in case of disaster and crisis/emergency situations in the energy companies of the energy sector;
- takes decisions for undertaking specific actions for controlling the disaster or the crisis/emergency situation and proposes them to the Minister of Energy and, when necessary, to the NDPS.
- organizes the interaction of the Ministry of Energy with the structures of the Single Rescue System of the country (DG Fire Safety and Protection of the Population - Ministry of Interior, regional directorates of the Ministry of Interior, Bulgarian Red Cross, ministries and

departments, municipal staff for disaster protection, emergency medical care establishments in the area of the disaster, etc.) in carrying out the measures for protection in case of disasters and the implementation of the tasks and measures for disaster management.

- organizes, coordinates and controls the actions carried out by the formations of the Energy Sector, an integral part of the power system, for the implementation of the tasks and measures for disaster protection;
- is responsible for the implementation of the assigned obligations arising from the implementation of the National Preventive Disaster Protection Plan and the Action Plan of the ME, in constant cooperation with the National Staff, the Regional Cooperation Center, the EC structures;
- proposes to the Minister of Energy solutions for managing crisis/emergency situations and eliminating the consequences of the disrupted electricity supply;
- makes proposals to the Minister for providing additional financial resources, fuel reserves and other resources for the activities for disaster protection and crisis/emergency management and for liquidation of the consequences;
- proposes estimates for the allocation of reserves of energy and other resources in a crisis/emergency situation and the introduction of a restrictive regime for the supply of electricity, thermal energy or natural gas in cases where it is necessary to limit or interrupt the supply for a period of time longer than 48 hours throughout the country;
- proposes measures to support the supply of electricity to neighbouring countries (Member States of the European Union) or cooperation with the Member States of the European Union;
- prepares summary inquiries and reports to the Minister of Energy and/or the NDPS on the changes in the situation and the course of implementation of the restoration/rescue activities.

The work of the Departmental Staff is supported by the operational duty officers in the Ministry of Defence and the experts from the Directorates Security of Energy Supply and Crisis Management. In carrying out its activities, the Departmental Staff, depending on the situation, may operate in normal and crisis mode according to the rules approved by the Minister of Energy.

In case of absence of any of the members, his deputy is appointed by the respective administrative unit, who participates in the work of the Departmental Staff. If necessary, by decision of the Chairman of the Departmental Staff, other employees may be included in the Staff.

- SIAP - The transmission system operator appoints a permanent Staff for the Implementation of the Action Plan (SIAP), which is responsible for the implementation of the Plan on its part. The scheme of notification, in case of occurrence or expectation of occurrence of crisis level, of the Staff is in accordance with the order of the Executive Director of the operator.

5. Stakeholder consultations

Ministry of energy;

Energy and Water Regulatory Commission;

The Electricity System Operator;

Electricity distribution companies;

The competent authorities pursuant to Regulation 2019/941 in the Hellenic Republic and Romania.

6. Emergency tests

Due to the fact that not all neighbouring countries of Bulgaria are members of the EU (Turkey, Serbia, Republic of North Macedonia) and have not made commitments to meet the requirements of Regulation 2019/941, no regional emergency tests have been conducted so far concerning power supply crises. In case agreements are reached for such regional tests, their essence and results will be reflected in the next update of the Plan.

However, in accordance with the requirements of Regulation (EU) 2017/1485 establishing a guideline on electricity transmission system operation (SOGL), ESO EAD conducts annual trainings and tests of RDC and NDC dispatchers in order to refresh and improve knowledge and skills needed to respond adequately to a wide range of emergencies. For this purpose, some of the tests are conducted on the so-called dispatcher training simulator (DTS).

DTS is part of the information and management system of the NDC. With the conduct of the trainings, the dispatchers are trained for actions in normal and emergency operational situations, provided for in the Defence Plan and the Severe Accident Restoration Plan. Some of the main options are as follows:

- Training and coaching of new dispatchers for operational management, work with software applications and AGC (Automatic Generation Control) functions of the model of the power system which simulates the real power system;
- Training and coaching of dispatchers preventively for the management of the energy system in emergency situations and recovery actions;
- Facilitates the development and testing of new applications and modification of the energy system;
- Introducing dispatchers to new applications and modification of the energy system;
- Provides training and analysis of dispatch responses to various events and restrictions;
- Provides training and analysis of dispatching skills for working with procedures for emergency restoration of the power system in case of complete or partial separation.

LIST OF USED MATERIALS

1. Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector, repealing Directive 2005/89/EC;
2. Commission Regulation (EU) 2017/2196 establishing a network code on electricity emergency and restoration;
3. Regulation (EU) 2017/1485 establishing a guideline on electricity transmission system operation;
4. Rules on Power Grid Control;
5. Policy on Emergency and Restoration, SAFA of ENTSO-E.
6. Policy 5: „Emergency Operations" of ENTSO-E
7. Power System Defence Plan of the Republic of Bulgaria developed by Electricity System Operator EAD;
8. System Restoration Plan of Bulgaria after severe accidents developed by Electricity System Operator EAD.