MEKH
Hungarian Energy and Public Utility Regulatory Authority

RISK PREPAREDNESS PLAN

Developed in accordance with Article 10 of the Risk Preparedness Regulation

Final version
Date: 4 January 2022

Clean energy, sustainable environment

Table of Contents

Introduction

The purpose of this document is to present the risk preparedness plan of the Hungarian Energy and Public Utility Regulatory Authority (hereinafter: **MEKH** or the **Authority**) based on the regional and national electricity supply crisis scenarios, in accordance with Article 10 of Regulation (EU) No. 2019/941 of the European Parliament and of the Council on electricity sector risk preparedness and repealing Directive 2005/89/EC (hereinafter: **Risk Preparedness Regulation**), which entered into force on 4 July 2019.

The ENTSO for the electricity industry (hereinafter: **ENTSO-E**) has prepared a summary document of regional electricity crisis scenarios based on data provided by transmission system operators (hereinafter: **TSO**) and based on the requirements set out in Article 6(2) of the Risk Preparedness Regulation, and on 7 September 2020 it submitted the regional electricity supply crisis scenarios to the TSOs concerned, the Regional Coordination Centres (hereinafter: **RSC**), the competent authorities and regulators, and the Electricity Coordination Group (hereinafter: **ECG**).

According to the process described in the Risk Preparedness Regulation, ENTSO-E, in cooperation with the Member States and the ECG, has identified and assessed 31 electricity crisis scenarios.

In accordance with Article 7(2) of the Risk Preparedness Regulation, the Authority put forward its proposal for national crisis scenarios for industry consultation between 14 and 28 December 2020, which is also in line with the regional electricity crisis scenarios identified by ENTSO-E.

As a result of the consultation, the Authority identified 18 relevant national scenarios, which have been addressed in the risk preparedness plan presented in this document.

The purpose of the risk preparedness plan is to describe the preventive, preparedness and management procedures to be implemented in the event of a potential electricity crisis.

1 General information

The risk preparedness plan was compiled by the Authority, taking into account the requirements of the Risk Preparedness Regulation.

1.1 General information in relation to the Hungarian Energy and Public Utility Regulatory Authority

Full name: Hungarian Energy and Public Utility Regulatory Authority

Registered office: H-1054 Budapest, Bajcsy-Zsilinszky út 52.

President: Péter János Horváth

1.2 Member States in the Region

The region concerned is the Central Europe SOR (System Operational Region) approved by the decision of the Agency for the Cooperation of Energy Regulators (hereinafter: **ACER**) (DECISION No. 10/2020).

Accordingly, the Member States in the region concerned are: Austria; Belgium; Czech Republic; France; the Netherlands; Croatia; Poland; Luxembourg; Germany; Italy; Romania; Spain; Slovakia; Slovenia; and Portugal

For third countries (non-EU Member States) in the region: Serbia, Ukraine.

2 Summary of Electricity Supply Crisis Scenarios

In accordance with the powers conferred on it by Article 29 of Act CI of 2019 on Electricity Amending Certain Energy-Related Acts for the Purpose of legal Harmonisation, which amended Act LXXXVI of 2007 and entered into force on 1 January 2020, the Authority, as the competent authority designated according to Article 3(1) of the Regulation and acting in respect of Article 4, Article 6, Article **7(1) and (2)**, Article 10, Article 12(3), Article 13 and Article 17 of the Regulation, is responsible for determining the most relevant national electricity supply crisis scenarios.

In accordance with Article 7(2) of the Risk Preparedness Regulation, the Authority put forward its proposal for national crisis scenarios for industry consultation between 14 and 28 December 2020, which is also in line with the regional electricity crisis scenarios identified by ENTSO-E.

As it does not consider it necessary to propose any scenarios in addition to the list of regional scenarios established by ENTSO-E on the basis of the methodology developed and adopted under Article 5 of the Regulation and taking the opinions received in response to the consultation into account, the Authority selected the relevant national crisis scenarios from the regional list of scenarios, taking the assessment criteria of the methodology referred to above into account, and determined them on 21 January 2021, in accordance with Article 7(1) of the Risk Preparedness Regulation.

The following figure lists the national crisis scenarios identified by the Authority, where the different colour codes indicate the relevance of the particular crisis scenario (red = high-priority; yellow = significant).

Relevance: relevance is a complex indicator of two factors. One factor measures the severity and extent of the consequences of the scenario (insignificant < low < high < critical < disastrous), while the other factor measures the probability of occurrence (none <low <high). The measurement of probability and impact in the indicator is complemented by the examination of cross-border interactions.

Name of the national electricity supply crisis scenario	**Relevance**
Cyber-attacks against the critical information technology infrastructure of a system operator and the key system user (TSOs; DSOs; power plants and large industrial customers)	
Physical attack on critical assets/equipment	
Physical attack on the control centre	
Hostage taking/threatening/blackmailing of senior personnel	
Insider attack	
Storm	
Heavy rainfall and flooding	
Extreme winter weather event	
Fossil fuel shortages (including natural gas shortages)	
Loss of critical information and communication technology infrastructure required for real-time or near real-time electricity system management	
Unplanned flows due to physical flows that do not follow market-scheduled flows	
A significant industrial or nuclear accident with prolonged nuclear or toxicological contamination, which may result in long-term loss of personnel (months or years)	

Extraordinary estimation error in renewable energy generation	
Pandemic	
Heatwave	
Dry period	
Earthquake	
Forest fire	

2.1 Cyber-attacks against the critical information technology infrastructure of a system operator and the key system user (TSOs; DSOs; power plants and large industrial customers)

Relevance: high-priority

In this scenario, the information communication systems of TSOs, distribution system operators (hereinafter: DSOs), power plants or large industrial customers are affected by a cyber-attack (e.g. central SCADA system; sub-station SCADA control; EMS; central power frequency controller; data loggers; management tools; power plant control systems; office IT tools).

An attacker may successfully access critical ITC systems, gain access to use the systems and manipulate the settings, input and output data and instructions of command and control devices, and may be able to deny access to authorised employees.

The attack may lead to unscheduled outages of transmission lines, transformers and power plants, which may lead to the overloading of other network elements and loss of loads. Cross-border effects may also occur. The scenario may also affect the business conduct of market participants.

2.2 Physical attack on critical assets/equipment

Relevance: high-priority

In this scenario, a physical attack hits a transmission line, a transformer, a substation, a power plant or a data centre.

The attacker destroys the technical equipment of the TSO, DSO or power plant. An attack may make it impossible to apply or restore the N-1 principle. Electricity transmission may also become impossible. The attack may cause power outages in some areas. The recovery of devices affected by the attack can take a long time. Cross-border effects may also occur. The scenario may also affect the business conduct of market participants.

2.3 Physical attack on the control centre

Relevance: high-priority

In this scenario, a physical attack hits the control room or the backup control room of the TSO, DSO, or large power plant. The attacker's goal is to destroy the control room or the backup control room. The system operator is unable to manage the network and balance the load of power plants, and the exchange of cross-border schedules between TSOs becomes impossible. The attacker may shut down the plant. The electricity system becomes unmanageable. Energy supply and delivery must not be interrupted, but the security of supply is compromised because the ability to respond effectively to any grid incident is severely limited. Cross-border effects may also occur. The scenario may also affect the business conduct of market participants.

Hostage taking/threatening/blackmailing of senior personnel

Relevance: significant

In this scenario, a senior staff member is forced to take action that undermines the stability of the system. The senior staff member may be a system operator, an ITC specialist, a staff member with access to critical systems and applications, or senior management. Forced by the attacker, an employee has access to control the network and can cause unscheduled outages. The TSO, DSO or power plant loses the ability to have full control over system management or plant management. The security of supply may be compromised and load shedding may occur. Cross-border effects may also occur. The scenario may also affect the business conduct of market participants.

2.5 Insider attack

Relevance: significant

In this scenario, an employee or subcontractor initiates a sabotage event using physical intervention or misuse of ITC systems. An employee or subcontractor may thus take control of the network or cause physical damage to the equipment. The TSO, DSO or power plant loses the ability to have control over system management or plant management. The security of supply may be compromised and load shedding may occur. Cross-border effects may also occur. The scenario may also affect the business conduct of market participants.

2.6 Storm

Relevance: significant

In this scenario, a thunderstorm is predicted and security interventions are ordered. The intensity and extent of the predicted storm will increase sharply in the last hour. As an example, it sweeps from Western to Eastern Europe with an average wind speed of 150 km/h and gusts of 200 km/h. Local eddies, gusts of wind and lightning occur, which also affect the electricity infrastructure. The storm lasts for three days and affects several network elements at once. Transmission lines and substations are damaged, the automatic protection against lightning is activated, cross-border lines reach their maximum load, transmission capacities may be limited, and island operation or load shedding and

consumer load limitation may take place. Power plant generation may drop due to the curtailment of wind power generation for safety reasons, and system interconnectors, distribution network elements and distribution network generation resources may be lost. Cross-border effects may also occur.

2.7 Heavy rainfall and flooding

Relevance: significant

In this scenario, typically in the spring, a rapid rise in temperature or prolonged rain will raise water levels. Heavy rain lasting for several days may cause flooding at substations or power plant sites. Landslides may also occur. Power plants may shut down and substations may be de-energised. Asset restoration can only begin once the water has receded and may then take up a longer time period. The foundations of transmission line pylons may also be weakened. The flooding makes recovery work more difficult and slower for maintenance staff. Defence works, eventually including river dams, weirs and hydroelectric power stations, may also be damaged, and a possible breach of the dam may cause the river to alter its course and damage the surrounding areas. Unplanned loss of load may occur in areas where flooding causes damage to transmission, distribution or power plant equipment. Heavy rainfall may make it difficult to maintain the continuity of surface fossil fuel mining. The availability of balancing regulatory reserves and power plants that may be involved in redispatching may decrease. Cross-border effects may also occur.

2.8 Extreme winter weather event

Relevance: significant

In this scenario, there is a high system demand and transmission demand, with below-average winter temperatures, and heavy snowfall. Low temperatures are also associated with high power consumption. Damp and windy weather is accompanied by the icing of the wires and transmission line poles. Snow is formed on the trees near the transmission lines, and there is a risk of avalanches in the mountains. Power line poles may be damaged and power lines may fail. A radial-connected network may develop. Restoration and the deployment of maintenance staff is delayed due to the dangers posed by bad weather and possible traffic difficulties. Load shedding may occur; transmission bottlenecks may take place and power plant generation may need to be instructed to divert. Cross-border effects may also occur.

2.9 Fossil fuel shortages (including natural gas shortages)

Relevance: high-priority

The scenario is characterised by high domestic fuel consumption and low inventories during the period under review. Fossil fuel production is interrupted for an extended period of time, the fuel supply system is shut down for technical reasons or malicious activity, and fuel supply is interrupted due to commercial, political or weather conditions. The risks are different if the scenario is due to the interruption of production, malicious activity, a transit barrier, and/or other (political, commercial, etc.) reasons. In the case of imported fuel, transit countries introduce restrictions to ensure their own supply. The deficiency cannot be replaced in an alternative way. Generation in fossil fuel-independent power plants may be given priority load sharing, and generation from fossil fuel-using power plants is limited for fuel economy reasons. There may be a complete shutdown of power plants. The availability of backup

capacities becomes limited, and voltage stability and inertia problems can occur in the system. Due to the lack of fossil fuels, supply in the markets of system-level services may decrease, and it may be necessary to include renewable energy generation in the regulation, so production of renewable energy generation may be reversed, and import opportunities may decrease. A Rotating Load Shedding Systemmay be adopted. Cross-border effects may also occur. The scenario may also affect the business conduct of market participants.

2.10 Loss of critical information and communication technology infrastructure required for real-time or near real-time electricity system management

Relevance: significant

In this scenario, a significant part of the telecommunication infrastructure required for electricity market operation or management is lost or the information communication systems necessary for real-time system operation and market operation are lost for technical reasons. Control of the electricity system becomes impossible or severely limited. Affected system operators and market participants use fall-back procedures, which in some cases do not have all the necessary functionalities (possibly affected by the outage). Until control is restored, the system may be subject to further disruptions and switching to backup procedures, in addition to human failure. Forced (but controlled) disconnection may be used as a safety intervention, possibly including emergency disconnection of consumer or production assets. Market participants may suffer financial losses due to incorrect information or the unavailability of market data. Decisions made by market participants based on misinformation may further aggravate the state of the system. Instead of a market-based load distribution, load may be distributed by and according to transmission system operators. Cross-border effects may also occur.

2.11 Unplanned power flows due to physical flows not following market-scheduled flows

Relevance: significant

In this scenario, the system is overloaded, bottlenecks occur on internal and cross-border network elements, and unscheduled outages take place. Higher-than-estimated power flows occur, partly due to higher renewable-based power plant production, and partly due to unusual production patterns due to national or international redispatching measures. The rate of unscheduled flows is high, in addition to the power flows from the capacities offered from the coordinated capacity calculation. The N-1 safety principle cannot be upheld, and thus safety interventions are required. Unscheduled outages of network elements can occur and power outages may occur. Cross-border effects may also occur.

2.12 Significant industrial or nuclear accident with long-term nuclear or toxicological contamination, which may result in long-term loss of personnel (months or years)

Relevance: significant

In this scenario, a major industrial accident occurs (radioactive contamination escapes from the safety zone of a nuclear power plant; an explosive or toxic substance leaves a chemical plant) for any reason (including technical failure; earthquake; sabotage; terrorist attack; human error or failure). Plant management cannot be ensured in the area affected by contamination. The control room staff (for any actor in the electricity supply chain) are directly involved and are unable to perform their duties for long

periods of time. Power plant outages may occur, and restoration cannot be performed due to limited accessibility of the area. As a result of contamination, power plants can be expected to shut down due to contamination in addition to the outages. Maintaining system balance requires increased measures, making planned and emergency maintenance impossible and increasing the risk of human error. In the case of radiation contamination, the affected part of the electricity infrastructure becomes inaccessible for years or decades and, in the case of industrial chemical pollution, for weeks or months. Cross-border effects may also occur. The scenario may also affect the business conduct of market participants.

2.13 Exceptional estimation error in renewable energy generation

Relevance: significant

In this scenario, there is a striking and significant discrepancy between the forecast and the actual amount of electricity generation from renewable (solar and wind) energy sources. The source of the forecast error may be from the erroneous estimation of input data or a sudden and unexpected change in the weather. With a low system load level, the severity of the scenario may increase. The difference between the planned and the actual renewable generation may exceed the reserve sizing limit. Unexpected surplus or decrease of production leads to unexpected and sizeable load reduction or increase needs. The TSO may exhaust its available security interventions. Adherence to the N-1 safety principle may be compromised, and the interruption of renewables production may lead to load shedding. Cross-border effects may also occur.

2.14 Pandemic

Relevance: high-priority

In this scenario, an infectious disease spreads locally or across Europe, with pandemic-like proportions. The disease spreads internationally. TSO plant management personnel may also be affected. Infections can also occur in DSO and power plant personnel, resulting in staff shortages. Epidemiological measures may impose further restrictions, which may affect the conditions and circumstances under which plant management is carried out. Labour and staff shortages could lead to unplanned plant closures. The epidemiological measures can also impede maintenance or inspections, leading to unplanned shutdowns of power plants again. The performance of field work by TSO may also be subject to restrictions. The possible loss of central control staff jeopardises the efficient performance of system management tasks. Even after the introduction of precautionary measures, some staff may be absent from work for personal or family reasons. The disconnection of some pre-selected network elements, power plant failures, loss of reserves, and balancing difficulties may take place, which increase the costs of system management. If the economy comes to a standstill, low consumption values may increase voltage levels and increase the chance of human error or omission. There may also be generation outages. Staff shortages may lead to a reduction in the quality of maintenance work, the need to reschedule and sometimes postpone maintenance work, and disruptions in the supply chains for spare parts and other equipment. Cross-border effects may also occur.

2.15 Heatwave

Relevance: high-priority

In this scenario, heat waves form in most of Europe, with heat peaks lasting for at least ten days. Water levels in most European rivers fall to low levels due to drought. At the same time, demand for electricity increases, especially in southern Europe, and high power flows develop. Temperatures in reservoirs and streams rise, which could limit water-cooled power plants. The lack of rain further reduces the water level of rivers and reservoirs. Generation by hydropower and wind farms is also declining. Imports and transmission capacity are reduced due to the reduced thermal load capacity of transmission lines. Internal and cross-border bottlenecks may develop. Some power plants are not operating due to scheduled maintenance. A heatwave can have an impact on the security of supply, with power plants going offline or production being reduced. Some network elements may be overloaded, and compliance with the N-1 operational safety principle may be compromised. The increased use of air conditioners also causes an increase in electricity demand. A source compliance problem may arise. There may also be load limitations and production losses. Cross-border effects may also occur.

2.16 Dry period

Relevance: high-priority

This scenario presumes a prolonged period of extreme drought (with hardly any rain for weeks) and hydroelectric reservoirs are almost completely depleted. Water levels in most European rivers fall to low levels due to drought. Low water levels are associated with low hydropower generation. Thermal power plants using water cooling may also reduce their generation and possibly shut down. Production capacities and import opportunities may be reduced during peak periods. There may be a source adequacy problem and scarcity. Consumption may be recharged at certain times. During some hours of the day, a Rotating Load Shedding Systemmay apply. The effects may be felt simultaneously in several countries and regions of Europe. Cross-border effects may also occur.

2.17 Earthquake

Relevance: high-priority

In this scenario, earthquakes can be predicted seconds before they occur, so the TSO does not have time to prepare for the event in advance. An earthquake of significant magnitude occurs, and may damage transmission network and power plant infrastructures. Depending on the impact, large power plant or transmission network outages may occur. Damage to the control centre may also affect the operational safety of system control. Transmission network capacity and system balancing capacity may be reduced. Uniform damage to hydropower plants or other power plants may result in a reduction in resources suitable for system-wide service. Load limitation may also be ordered during peak hours. The effect on the transport infrastructure may also increase recovery time. Cross-border effects may also occur.

2.18 Wildfire

Relevance: significant

In this scenario, prolonged periods of drought dry out forested, heatherland, grassland or bushland landscapes. Wildfire ignition and spread starts with the interaction of the dry season and windy weather. The fire that has started cannot be brought under full control for weeks. Uncontrolled wildfires may result in outages in power plants and the failure of transmission or distribution network assets. This may

also compromise compliance with the N-1 operational safety principle, which may eventually lead to cascade (chain-like) events. Network outages are due to wildfires or the planned intervention by extinguishing authorities. Physical damage to transmission line poles and wires may also occur. Load loss and load limitation may take place. A state of scarcity may arise, including in balancing regulatory markets. Network maintenance may also need to be rescheduled. Cross-border effects may also occur.

3 Roles and responsibilities of the competent authority

The Authority shall exercise the powers conferred on it by Section 29 of Act CI of 2019 amending Act LXXXVI of 2007 on Electricity (hereinafter: **Electricity Act**) amending certain energy-related acts for the purpose of legal harmonisation, which entered into force on 1 January 2020, as a competent authority designated under Article 3(1) Regulation (EU) No. 2019/941 of the European Parliament and of the Council on Risk Preparedness in the Electricity Sector and Repealing Directive 2005/89/EC (hereinafter: **Risk Preparedness Regulation**), acting in accordance with Articles 4, 6, 7(1) and (2), 10, 12(3), 13 and 17 of that Regulation, and shall determine the most relevant national electricity supply crisis scenarios in accordance with Article 7(1) of the Risk Preparedness Regulation.

According to Section 139/A of the Electricity Act, the competent authority:

*"Section 139/A * (1) With the exception of paragraph (2), the Minister shall act as the competent authority for the provisions of Regulation (EU) No. 2019/941 of the European Parliament and of the Council.*

(2) Articles 4, 6, 7 (1) and (2), 10, 12 (3), 13 of Regulation (EU) No. 2019/941 of the European Parliament and of the Council, and Article 17 shall be performed by the Authority.

(3) The Authority shall make a professional proposal to the Minister in relation to the tasks referred to in subsection (1). "

Government Decree No 280/2016. (IX. 21.) on Measures to be Taken in the Event of a Major Disturbance to the Electricity System and an Electricity Supply Crisis (hereinafter: **Government Decree**) sets out the role of the competent authorities and the bodies involved in the prevention of and in the event of an electricity crisis.

According to the Government Decree, the Authority is responsible for the designation of essential users, the approval of the Rotating Load Shedding Systemand the Crisis Plan.

In order to monitor the implementation of the Risk Preparedness Regulation and the Risk Preparedness Plan, the Authority is entitled to request information from the Crisis Working Committee on the performance of the Crisis Working Committee's tasks in the event of a crisis scenario described in Clause 2, as well as information from the TSO, DSO and producer affected by the occurrence of the crisis scenario r on the implementation of the tasks prescribed in the risk preparedness plan, including preventive and crisis management measures.

In accordance with Article 14(1) of the Risk Preparedness Regulation, where a seasonal conformity assessment or other qualified source provides specific, serious and reliable information to the effect that an electricity supply crisis may occur in Hungary, the Authority shall assist the competent authority in providing early warning to the Commission without undue delay and to the competent authorities of the Member States in the same region and, if they are not located in the same region, of directly interconnected Member States

In the event of an electricity supply crisis, the Authority shall, in accordance with Article 14(2) of the Risk Preparedness Regulation, assist the competent authority, after consulting the transmission system

operator concerned, to notify the electricity supply crisis and inform, without undue delay, the competent authorities of the Member States in the same region and, where they are not in the same region, the competent authorities of the directly interconnected Member States, as well as the Commission.

In accordance with Article 17(1) of the Risk Preparedness Regulation, the Authority shall send an *ex post* evaluation report to the Electricity Coordination Group and to the Commission no later than three months after the end of the electricity supply crisis.

3.1 Duties and responsibilities of other participants specified in the Government Decree

Pursuant to Section 8 (1) of the Government Decree, the TSO shall establish a Crisis Working Committee (hereinafter: **CC**), with tasks set out in the Government Decree.

The chairman of the CC shall be the CEO of the TSO, and its members include two representatives of the generating licence holders and two representatives of the DSOs, and one representative each of the TSO, the nuclear power plant, the universal service providers and the electricity traders.

The CC is responsible for commenting on the Electricity Crisis Plan developed by the TSO and approved by the Authority.

The transmission system operator shall elaborate a Crisis Plan, mandatorily including, inter alia, the means and procedures for informing public bodies, users and licence holders on forecasting the curtailments needed to reduce consumption and on the curtailments in order to prepare the public, system users and licence holders.

The tasks of the TSO are to the provision of the necessary reserves for the security of supply, the management of the operation of the system, and the checking of proper preparation. To take efficient measures towards all participants in the electricity market to prevent major disturbances and crisis situations, to develop a Rotating Load Shedding System (hereinafter: **RLSS**) in cooperation with the distribution network licence holders, to coordinate the installation of automatic limiting and disconnection devices, to perform crisis simulation exercises, and to initiate public information.

The DSO is tasked with proposing the classification of users as essential users, cooperating with the TSO in the development of the RLSS, updating the RLSS-related user register, procuring, installing, operating, maintaining and monitoring automatic limiting and disconnection equipment and providing the TSO with data to help establish the necessary measures to prevent a crisis. The DSO shall develop a distribution crisis plan for its own territory in accordance with the Government Decree.

Producer, trader and universal service licence holders are responsible for providing the transmission system operator with data to help establish the measures necessary to provide for surplus electricity and to restore the balance of consumption in the event of a power shortage in the electricity system in order to prevent a crisis.

4 Procedures and measures in the event of an electricity supply crisis

The procedures and measures presented in this chapter have been developed on the basis of EU and Hungarian legislation and are already applicable if necessary.

Irrespective of the cause of the crisis, most of the procedures and measures are the same and are generally presented by the Authority. The specific procedures and measures to be applied in each crisis scenario are described by the Authority in Section 4.5.

4.1 National procedures and measures

National procedures and measures have been developed on the basis of the following EU and national legislation:

Hungarian legislation and regulations:

- Act LXXXVI of 2007 on Electricity,
- Government Decree No. 280/2016. (IX. 21.). on Measures to be Taken in the Event of a Major Disruption of the Electricity System and a Crisis in the Supply of Electricity.
- Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Installations,
- Electricity supply codes: Operational Code (hereinafter: **OC**), Commercial Code (hereinafter: **CoC**), International Operation and Commercial Code (hereinafter: **IOCC**), Distribution Code (hereinafter: **DC**),
- Crisis Plan for the Prevention and Mitigation of an Electricity Crisis,
- System recovery plan.

International legislation and methodologies:

- Commission Regulation (EU) 2017/2196 establishing a network code on electricity emergency and restoration (hereinafter: "**ER NC**"),
- Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation (hereinafter: **SO GL**).

Pursuant to Section 14 of the Electricity Act and the ER NC, the TSO is responsible for developing the Crisis Plan, the System Recovery Plan and related methodologies. These documents are valid for all relevant market participants and are summarised below.

Crisis plan:

The Crisis Plan contains measures to prepare society, system users and licence holders to deal with a crisis situation, to ensure the fullest possible coverage of users, to specify the cooperation, division of tasks, responsibilities and obligations of the organisations managing the protection and those involved in the protection. It sets out how public authorities, system users and licence holders are to be properly and jointly informed.

The procedures to be followed in the event of an electricity supply crisis, including the related schemes for the flow of information, are set out in the Crisis Plan.

Procedures to be followed in the event of electricity supply crisis:

In the event of an electricity supply crisis as defined in the Electricity Act and the Government Decree, the Government is responsible for the management of the protection measures pursuant to Section 2(3) of the Government Decree. In this context, the Government is entitled to issue a decree providing for the introduction of emergency measures.

1. The transmission system operator shall act in accordance with its rights and obligations to remedy the significant disturbance until the Government takes action. Following the declaration of a state of national crisis, it shall issue its measures on the basis of and in accordance with the regulations or instructions issued by the Government concerning the state of national crisis.

2. In the event of a crisis, unless otherwise provided by the Government or legislation, the TSO and the Authority shall act in accordance with the rules for the management of major disturbances set out in the Crisis Plan.
3. Electricity generation licence holders shall perform the tasks prescribed for them in the event of a crisis in the Government Decree on Crisis Situations and in the Crisis Plan and its annexes in the order and to the extent determined by the transmission system operator.
4. In the event of a crisis, the CC shall meet as necessary in order to assess the situation and to coordinate the activities of system users and public bodies involved in crisis management.
5. The information system shall be operated by the transmission system operator for the purpose of providing information to public authorities and society, and for providing data for the continuous assessment of the situation.
6. The provision of data shall be performed by the operational management personnel of the electricity industry licence holders, with the content and frequency determined by the transmission system operator in accordance with the given situation.
7. In order to reduce the capacity deficit in the electricity system, the system operator shall initiate extra electricity generation and extra imports with the competent licence holders.
8. In a crisis situation, electricity trading shall continue in line with the Crisis Plan.
9. The transmission system operator may, in order to maintain the balance of power of the electricity system, order distribution network licence holders to reduce the user load through the prepared RLSS. User curtailments that depend on the degree of power failure shall be ordered and implemented in accordance with the prescribed RLSS procedures.
10. In the event of a crisis situation ending, the transmission system operator shall instruct the distribution system licence holders to reconnect users and to restore regular operation. It shall report to the Minister and to the Authority on the implementation of the measures.
11. Following the end of the crisis situation, the transmission system operator shall prepare a summary report with the involvement of the members of the CC, which shall then be sent to the Authority. The Authority must inform ECG at the earliest possible date, but in any case within three months of the end of the electricity crisis.

Schemes related to the flow of information:

The use of the national information system in the event of a crisis shall be coordinated centrally by the transmission system operator. The Secretary of the CC and the Security Manager of the Transmission System Operator shall liaise with public bodies as necessary.

In the event of a crisis, the transmission system operator shall keep the competent Minister and the President of the Authority informed of the system-wide fuel and performance situation. It shall report on events that may trigger a crisis situation, and in the event of a crisis, it shall communicate the expected duration, consequences, measures taken to resolve it and their expected impact. It shall report to the competent Minister and the President of the Authority about the end of the crisis.

In the event of a foreseeable crisis, the transmission system operator shall inform the distribution licence holders and the central head office of the Ministry of the Interior Disaster Control Directorate 48 and 24 hours before user curtailments. In the event of shorter foreseeability, forecast information must be provided without delay. The transmission system operator shall again notify the distribution network licence holders and the central head office of the Disaster Control Directorate of the Ministry of the Interior of the predictable user curtailments at least 1 hour before the implementation.

In the event of an unforeseen (failure-related) restriction, the transmission system operator shall immediately inform the central head office of the Disaster Control Directorate of the Ministry of the Interior immediately after the curtailment has been carried out.

The National Dispatcher Service of the transmission system operator (hereinafter: NDS) shall maintain contact with the system users. The dispatcher services of the distribution and generation licence holders shall have direct contact with the NDS.

In the event of a crisis, the licence holders shall contact the competent County Disaster Control Directorates (in the case of Budapest: the Metropolitan Disaster Control Directorate). The transmission of information to local public bodies (County Protection Committees, Local Governments, Professional Fire Brigades, in the case of Budapest: Budapest Fire Brigade) falls into the competence of the County Disaster Management Directorates (in the case of Budapest, the Budapest Disaster Management Directorate).

System protection plan:

The aim of the plan is to prepare for and prevent the occurrence of possible major – even continent wide – system failures, and to prevent critical disruptions from worsening despite preventive measures. In accordance with the requirements of the Regulation, the two main groups of measures in the System Protection Plan are the Frequency Plan and the Voltage Plan, which specify specific intervention measures (automatic and manual) for when the frequency and voltage values are outside the prescribed operational safety limits. In addition to the two main groups of measures, the plan also includes provisions for lockout/tagout and for the automatic protection system, and provisions for the management of intersystem oscillations.

System recovery plan:

The plan shall include all system operator actions required to restore the regular operation of the electricity system following a major system failure or system breakdown.

The plan describes the steps that the TSO shall take to restore regular operation. System recovery methods:

- Building from top to bottom: in this case, recovery relies essentially on the neighbouring electricity systems.
- Building from bottom up: in this case, the recovery is essentially based on internal resources, by restarting black-start power plants.

Market suspension methodology based on ER NC:

It is also a basic premise in the market suspension methodology developed in relation to the ER NC and of the regulation that, as long as this does not jeopardise the operation of the electricity system, market processes must be maintained and the necessary conditions for their operation must be ensured. In the event that the electricity system is in an emergency, black-out or post-recovery state, or in the event of an IT or communication problem, the ER NC specifies the market activities that can be suspended in order to return to regular operational status as soon as possible. The market suspension methodology specifies the conditions under which the system operator may initiate the suspension of certain market activities, and the methodology also determines the scope of these activities. In order to ensure that only the necessary and sufficient market activities are suspended in a given situation, the methodology also presents the consequences of suspension. When national crisis scenarios set out in the risk preparedness plan actually take place, the state of the electricity system is also specified and, as a result, the necessary market interactions can be determined on the basis of the methodology. However, it is always worth examining these interactions in the context of the event that has materialised in order to ensure that only those market activities that are necessary and that only those activities that are helpful in the given situation and that are conducive to a solution are suspended. The methodology is part of the International Operational and Commercial Code, which is published on the TSO's website.

System states determined on the basis of SO GL:

Article 18 of the SO GL specifies the system states describing the operational status of electricity systems. Each system status is determined on the basis of specific operational safety indicators, which any TSO is able and obliged to monitor in order to establish the operational status of its own system properly and to interpret it clearly to other system operators. The primary means of sharing information on system states is the EAS system.

The regulation distinguishes five system states: normal, alarm, emergency, blackout, and recovery. The factors that fundamentally determine the state of a system are:

- power flows at baseline or in the N-1 case (taking the intervention measures into account)
- voltage values in ground state and in the case of N-1 (taking the intervention measures into account)
- steady-state system frequency deviation
- available effective and reactive power reserves
- the availability of tools, methods and facilities determined in accordance with Article 24 (1) of the Regulation
- introduction of a measure in a system protection plan
- rate of user outage
- implementation of the measure in the recovery plan.

Each TSO shall determine the system status of its transmission system during real-time operation, monitor key transmission system parameters based on real-time telemetry measurements or calculated values from its monitoring area, and perform periodic failover tests by monitoring specified transmission system parameters, comparing them with the operational safety limits set by the Regulation.

4.2 Preventive and preparatory measures

Licence holders must be prepared to deal with the electricity crisis, and their internal instructions shall include their responsibilities for crisis management.

If there is the risk that a crisis situation may evolve, and in the event of a crisis situation, it is the responsibility of the licence holders to provide the transmission system operator with appropriate information with the content, form and frequency determined by the Crisis Working Committee for the given situation.

Pursuant to Section 138(2) of the Electricity Act, system users shall perform the instructions of the transmission system operator and the distribution network licence holder in the event of a significant disruption of the electricity system, regardless of the rights and obligations contained in the contracts entered into.

Tasks of the transmission system operator related to preparing for a crisis and during a crisis:

The transmission system operator must be prepared to deal with the crisis. Its internal instructions must include the crisis management tasks of the transmission system operator.

In the event of a significant disturbance, the transmission system operator ó:

a) shall report to the Minister for Innovation and Technology and the President of the Authority and inform the members of the CC of the occurrence, cause and expected duration of the significant disturbance,

b) shall report the events that may trigger a crisis situation to the Minister for Innovation and Technology , the President of the Authority and the National Disaster Control Directorate of the Ministry of the Interior. It shall provide information on the expected duration of the crisis

situation, its expected consequences, the measures to be taken for recovery and their expected impact,

c) may initiate the convening of the CC,

d) shall inform users of the situation and its expected duration through mass communication; it may ask users for voluntary load reductions,

e) in order to eliminate the disruption and mitigate its consequences, the transmission system operator may issue instructions for the use of operational safety services and system reserves, for the increased use of power plants and for the use of international assistance,

f) may order a voltage reduction to reduce consumption, and

g) may apply load limitations to the extent necessary. It may order automatic (frequency-dependent) or frequency-independent load reductions for up to 6 hours. If the significant disturbance exceeds the 6-hour period, an RLSS must be ordered in order to minimise the damage at the social level,

h) shall performs settlement with the electricity supplied to and used by the grid during the period of significant disruption. During the financial settlement, the parties to the contract must take into account the prices included in the original agreements or in the agreements on the resources used to remedy the disturbance.

Generation licence holders' responsibilities in crisis preparedness and response to the crisis:

Generation licence holders must be prepared to deal with the crisis. Their internal instructions must include their responsibilities related to crisis management.

Generation licence holders must ensure that, in addition to ensuring the generation needs stipulated in their contracts, their fuel stocks meet the requirements of Decree No. 44/2002 (XII. 28) of the Minister of Economy and Transport *on the minimum level of fuel stocks and the stocking regime for power plants with a capacity of 50 MW and above* [Decree No. 44/2002 (XII. 28) GKM]. The transmission system operator shall be informed of the reduction of fuel stocks in accordance with this Regulation.

Generation licence holders shall inform the system operator without delay of any changes in their operating characteristics (primarily: minimum and maximum generation output, black-start capability, load change rate, partial operation, and possibility to resume from scheduled maintenance).

In the event of the risk of a crisis developing and in the event of a crisis:

a) it is the responsibility of producers to provide the transmission system operator with the appropriate information, with the content, and in the form and frequency specified by the CC for the given situation, in the event of a crisis,

b) generation licence holders shall be obliged to inform the transmission system operator of their normative and security fuel stocks and their expected development, as specified in Decree No. 44/2002 (XII. 28) GKM, at the frequency determined by the CC,

c) generation license holders shall be obliged to comply with the transmission system operator's request to increase electricity generation up to their available capacity,

d) in the event of a call issued by the transmission system operator to increase generation, the producers' safety energy stock may also be used. The relevant authorisation shall be issued to the licensee concerned by the President of the Authority,

e) the time limit for replenishing the safety stock shall be set by the President of the Authority,

f) generation licence holders shall update their operational features at the request of the transmission system operator (minimum and maximum generation output, black-start capability, load change rate, partial operation, possibility to resume from scheduled

maintenance). If these differ from the documents previously provided to the transmission system operator, the transmission system operator shall be informed of the changes without delay,

g) the nuclear power plant shall be obliged to prepare a restart plan in the event of a possible complete power failure and to review it regularly. When updating the restart plan, if it differs from the documents previously provided to the system operator, the system operator must be notified of the changes without delay.

Distribution network licence holders' responsibilities in crisis preparedness and response to the crisis:

The distribution network licence holder shall draft a crisis plan broken down into its own territory, taking Section 9 (3) of the Government Decree into account. This Distribution Crisis Plan is a separate document and is not identical to the Crisis Plan developed by the TSO.

In order to prevent and mitigate the crisis, it is the responsibility of the distribution network licence holder, at its own expense, under the coordination of the transmission system operator, to procure, install, operate and control automatic limiting and switching equipment (FILC (Frequency-independent Load Control) and FDLC (Frequency-dependent Load Control)).

Upon the instruction of the transmission system operator, the distribution network licence holder shall check the functionality of the control and shut-off systems. It shall inform the transmission system operator of the results of the inspection and take measures to rectify any eventual malfunctions within 15 days.

The distribution network licence holder shall register the users and lines falling within its territory, named in the RLSS and planned to be shut down. The transmission system operator shall be notified of any change in the functionality of the restriction systems if the extent of the change exceeds 10% of the capacity to be limited for the licence holder or 50% of the capacity within a given user group for more than 15 days.

If a crisis situation is imminent and in a crisis situation, distribution network licence holders shall:

a) provide the transmission system operator with appropriate information, with the content and in the form and frequency specified by the CC for the given situation,

b) provide information on the status of their network and the generation output status of small power plants operating on their network in the form and with the frequency specified by the transmission system operator,

c) call, via their plant operators, on the operators of small power plants operating on their territory to increase their generation,

d) suspend network maintenance on the instructions of the transmission system operator in order to create the network image that is closest to the regular connection regime,

e) on the instructions received from the transmission system operator, ensure their operators are prepared to perform user curtailments, and to notify users classified in the first stage of the restriction (or possibly further stages depending on the absence of performance),

f) notify the users of the foreseeable user outages within the framework of social information at the local level, while this is performed by the transmission system operator at the national level

g) ensure energy supply for the machines and equipment necessary for the medical treatment of disabled users (e.g. patients using ventilators or dialysis equipment) and for the maintenance of their vital functions in accordance with Section 35 of Government Decree No. 273/2007 (X.19.) on the implementation of certain provisions of Act LXXXVI of 2007 on Electricity.

Responsibilities of electricity trading and universal service provider licence holders in preparing for and responding to a crisis:

Licence holders must be prepared to deal with an electricity crisis, and their internal instructions must include their responsibilities for crisis management.

Tasks in the event of the risk of a crisis situation developing and in a crisis situation

a) It is the responsibility of the electricity trading and universal service provider licence holders to provide the system operator with appropriate information with the content, form and frequency specified by the CC for the particular situation.

4.3 Measures to mitigate electricity supply crises

Operation of the electricity market in the event of a crisis:

The suspension of contracts in electricity trade is not appropriate in the event of an electricity crisis. The best way to supply consumers with electricity is if the contracts remain in force and are fulfilled as far as possible.

Pursuant to Articles 36 and 39 of the NC ER, a methodology for the suspension and resumption of market activities by the TSO has been developed and approved by the Authority.

The organised electricity market shall notify the Members of the suspension of trading in accordance with the provisions of the Market Regulations, as soon as possible by means of a Market Notice.

Following the notification of the crisis situation, no auction will be held or continuous trading will be suspended. The organized electricity market shall notify its members by means of a Market Notice. This situation will continue until the transmission system operator provides official information that the crisis situation has been resolved on a lasting basis.

In accordance with the relevant regulations, the organized electricity market must submit a timetable to the transmission system operator for the transactions that have already been concluded at time of notification of the crisis situation, but have not yet been physically performed.

If, due to a lack of resources, an electricity trade contract becomes partially or temporarily unenforceable, the relevant balancing groups shall be supplied with energy by the transmission system operator (balancing energy), and its settlement must be subject to the rules of balancing energy settlement.

Following the resolution of the electricity supply crisis, the suspension of trading must be lifted upon the instructions of the transmission system operator:

a) if the Crisis Working Committee declares the crisis situation resolved no later than 35 minutes before the closing date of the day-ahead market order book specified in the Market Regulations on the given trading day and the daily cross-border capacity auction has taken place without any problem, trading may be resumed on the organised electricity market,

b) if the preconditions for trading are not met by the date defined above, trading may only be resumed on the trading day following the resolution of the crisis situation.

4.4 Load control procedures

In the Hungarian electricity system there are two types of restrictions:

1. Regulatory (foreseeable) electricity load control (Rotating Load Shedding System- RLSS)

Official electricity load control is ordered and lifted by the operational staff of the System Operator based on the decision of the Government or on the assessment of the current situation of the electricity system.
Notice to and the deactivation of the users affected by the restriction is performed by the District Dispatcher Service of the network licence holder for the given supply area.

The Rotating Load Shedding System: the procedure for determining the frequency of the disconnections in a scheduled manner relative to the electricity shortage and the frequency of the switch-offs in order to maintain a balance between the electricity source side and the consumption of electricity,

Principle of Rotating Load Shedding System: the disconnection of different groups of electricity users from the electricity supply at different times, on the basis of the principle of equal treatment and the principle of non-discrimination, in order to maintain the balance between the source side of electricity and consumption.

The RLSS shall be developed by the transmission system operator and approved by the Authority.

The purpose of the design of the RLSS is to exclude users in accordance with the principles of equal treatment and non-discrimination and to classify users into stages of exclusion according to pre-defined performance quotas.

In order to ensure that, in the event of a crisis, curtailments only affect the justified groups of users and are implemented within a reasonable period of time, the transmission system operator must develop the RLSS in cooperation with the DSOs.

In order to minimise damage during the RLSS, disconnection stages not exceeding 3 hours must be provided in each supply area.

The RLSS must be designed in such a way that essential users are not affected by the switch-off of the electricity supply to the extent that it is not necessary for the performance of their core business.

The **Authority designates essential users on the basis of the Government Decree**, taking into account that it may designate them in the following categories:

- The facility of the network licence holder specified in the Electricity Act that performs system control, operation control and troubleshooting.
- The facility of the transmission system operator pursuant to the Natural Gas Supply Act performing system control, operation control and troubleshooting (including gas receiving stations, pressure boosting stations, natural gas storage, metering and disconnection stations).
- Hydrocarbon transmission pipeline under the Mining Act.
- Priority defence facilities.
- The Ministry of the Interior National Directorate General for Disaster Management, the county (capital) disaster management control centre, and the county (capital) defence committee are located.
    - One refuelling station per company providing emergency fuel demand for the extraordinary regulation on the disaster protection and law enforcement agencies and managing the national strategic reserve.
- The national public service television and radio stations and their means of communication, and network equipment for the distribution of news by professional law enforcement agencies.
- Inpatient specialist care providers and other providers belonging to the health subsectors covered by the Act on the Identification, Designation and Protection of Vital Systems and Facilities.
- Public airport and air traffic control and safety equipment.
- Deep mining and radioactive waste storage.

- A facility providing controlled-circulation sewage transport and sewage treatment, and a pumping station for drainage during floods and inland water protection.

The Authority continuously fulfils its tasks related to the designation of essential users provided for in the Government Decree.

2. Emergency (unforeseen) electrical load control (and FDLC and FILC)

Types of emergency load control:

(a) frequency dependent load control (FDLC),

(b) frequency independent load control (FILC).

Implementation may be automatic (FDLC) or manual (FILC).

Frequency-dependent load control (FDLC) must be used to prevent the frequency from falling below a given value in the event of a breakdown involving a significant frequency reduction, or to increase the frequency to the level required for reliable operation of power plants.

The FDLC system must be graded and the delay times must be set to the value specified by the transmission system operator so that only user power proportional to the frequency reduction is switched off.

The frequency setting, delay time and amount of user power involved in the stages of the FDLC must be determined in consultation with other energy systems operating in parallel.

The transmission system operator may apply frequency-independent load control (FILC) in the event of a sudden major source-side power failure or loss of network transmission capacity and immediate action is required to offset its effects.

4.5 Additional national measures for each crisis scenario

In view of the most relevant national electricity supply crisis scenarios identified in accordance with Article 7 (1) of the Risk Preparedness Regulation as described in Chapter 2, the distribution system operator, the transmission system operator and the licence holder of a large power plant shall take the following preventive and crisis management measures in addition to taking the actions and fulfilling the obligations set out in Clause 4.1-4.4, Clause 4.5 and Clause 4.6:

4.5.1 Additional national measures for distribution network operators for each crisis scenario

Scenario	Existing measures	
	Preventive measures	**Crisis management measures**
1Cyber-attacks against the critical information technology infrastructure of a system operator and the key system user (TSO's; DSO's; power plants and large industrial customers)	The **Operator Security Plan** (OSP) includes security measures in the areas of physical security, information security and ongoing availability. The development of an **Information Security Policy** (ISP), which contains the information security controls according to the Act on Information Security, with special emphasis on the SOC (Security Operation Centre), CERT (Computer Emergency Response Team) operation, which detects and manages security events and incidents. **Crisis management regulation** The aim of the crisis management regulation is to adopt all the organisational measures that are intended to provide protection against crisis situations, and to develop precautionary measures and plans that enable rapid, effective and purposeful measures in crisis situations.	According to the OSP and ISP, and the crisis management regulation.
2 Physical attack on critical assets/equipment	Elaboration and operation of an **object security policy**, which sets out the basic principles of the physical safety	According to the Object Security and Property Protection Policies, the Fire and Property Protection Regulations and the Crisis Management Regulations.

	requirements applied, the supporting processes and actors and their areas of responsibility. Develop a **property protection policy** that describes what to do in the event of a physical attack and what procedure to follow. The property protection expectation of the distribution network operator aims to prevent the development of risks that pose a threat to its operation, management, security and protection of property. These apply respectively to measures - personal, technical and organizational - to reduce the effects of emergencies and to deal with property security incidents. Fire Prevention and Property Protection Policies and Plant Management Regulations	
3 Physical attack on the control centre	Elaboration of an Object Security Policy, The operation of a **Property Protection Policy** or according to the Fire Prevention and Property Protection Policy, the Plant Management Regulation, OSP, and ISP	According to the Object Security, Property Protection, Fire and Property Protection and Crisis Management Policies.
4 Hostage taking/threatening/blackmailing senior personnel	**Authorisation regulation and crisis management policy The distribution network operator's Crisis Management Directive and Authorisation Regulation.** The directive regulates the most important requirements for the management of crisis situations that deviate from regular operation.	According to crisis management policy. According to crisis management policy.
5 Insider attack	Regulation of permissions, logging, monitoring and creation of immediate exclusion possibilities according to the OSP and ISP.	Incident management processes as laid down in the ISP, Incident Management and Crisis Management Policy.

6 Storm	Updating the **Emergency Manual**. The Manual helps to eliminate the most common large-scale distribution network failures by, among other things, prescribing preparedness requirements, setting out the composition and working methods of the Emergency Committee, and specifying analytical and evaluation activities. **Procedure According to the distribution network operator's Crisis Management Directive** The policy regulates the most important requirements for dealing with crisis situations that deviate from regular operation. Supporting the management of an emergency situation and in accordance with the Operations Management Regulations	Operation in accordance with the Emergency Manual, Crisis Management Directive and Crisis Management Policy. Measures specified in the policy
7Heavy rainfall and flooding	Updating the **Emergency Manual**. The Manual provides assistance in the resolution of the most frequent and widespread distribution network disturbances by, among other things, prescribing the preparedness requirements, specifying the composition and working methods of the Emergency Committee, and describing the analytical and evaluation activities. **Procedure According to the distribution network operator's Crisis Management Directive**	Operation in accordance with the Emergency Manual, Crisis Management Directive and Crisis Management Policy. Measures specified in the policy

	The directive regulates the most important requirements for the management of crisis situations that deviate from regular operation. Supporting the management of an emergency situation and in accordance with the Operations Management Regulations	
8 Extreme winter weather event	**The distribution network operator's Crisis Management Directive** Winter preparation, provision of materials, protective equipment, operational changes, continuous monitoring and intervention. Supporting the management of an emergency situation and in accordance with the Operations Management Regulations	Operation under the Crisis Management Directive, Emergency Manual and Operation under the Crisis Management Policy. Measures specified in the policy
9 Fossil fuel shortages (including natural gas shortages)	Updating limitation sequences. FALC (Frequency-independent Automatic Load Control) and RSLS (Rotating Load Shedding System)which are used to ensure power balance. Operations Management Code	Control sequences, ordering the application of plans for running at peak capacity. Measures specified in the policy
10 Loss of critical information and communication technology infrastructure required for real-time or near real-time electricity system management	Conclusion of contracts for back-up transmission paths. Operations Management Code	Switching to other communication channels. Measures specified in the policy

11 Unplanned flows due to physical flows that do not follow market-scheduled flows	Conducting **preliminary investigations** of overloads, stress problems, system restoration and preparing measures for their occurrence. Operations Management Code	According to the action plans. Measures specified in the policy
12 A significant industrial or nuclear accident with prolonged nuclear or toxicological contamination, which may result in long-term loss of personnel (months or years)	Creating conditions for geographically separate operations, business continuity plans and alternative modes of operation to support the continuity of operations and availability in the event of the loss of real estate and physical resources.	Separate operation, according to crisis management regulations.
13 Out-of-specification estimation error in renewable energy generation	Updating limitation sequences. FALC (Frequency-independent Automatic Load Control) and RSLS (Rotating Load Shedding System), which are used to ensure power balance.	Control sequences, ordering the application of plans for running at peak capacity.
14 Pandemic	The development and operation of a **pandemic policy**, business continuity plans and alternative modes of operation to support the continuity of operations and availability in the event of the loss of human resources or Ordering pandemic stages and related measures and use of personal protective equipment against viral infections at work	According to pandemic regulations and crisis management regulations. Measures specified in the policy
15 Heatwave	**Preparation for the summer,** the provision of materials, protective equipment, plant status changes, and continuous training on what to do. **Crisis Management Policy of the Distribution System Operator.** Preparation for the summer, the provision of	Operation in accordance with the Emergency Manual or Crisis Management Directive and Crisis Management Regulations. Measures specified in the policy

	materials, protective equipment, plant status changes, and continuous tracking and intervention. Operations Management Code	
16 Dry period	Updating limitation sequences. FALC (Frequency-independent Automatic Load Control) and RSLS (Rotating Load Shedding System), which are used to ensure power balance. **Crisis Management Policy of the Distribution System Operator.** Updating limitation sequences. FALC (Frequency-independent Automatic Load Control) and RSLS (Rotating Load Shedding System), which are used to ensure power balance. Operations Management Code	Control sequences, ordering the application of plans for running at peak capacity. Measures specified in the policy
17 Earthquake	Updating the **Emergency Manual**. The Manual provides assistance in the resolution of the most frequent and widespread distribution network disturbances by, among other things, prescribing the preparedness requirements, specifying the composition and working methods of the Emergency Committee, and describing the analytical and evaluation activities. **Operator Security Plan** **Crisis Management Policy of the Distribution System Operator.** Supporting the management of an emergency situation	Operation in accordance with the Emergency Manual, the OSP, or the Crisis Management Directive and the Crisis Management Regulations. Measures specified in the policy
18 Wildfire	Updating the **Emergency Manual**. The Manual provides assistance in the resolution of the most frequent and widespread distribution network disturbances by, among other things, prescribing the preparedness requirements, specifying the composition and working methods of the	Operation in accordance with the Emergency Manual or Crisis Management Directive and Crisis Management Regulations. Measures specified in the policy

	Emergency Committee, and describing the analytical and evaluation activities. **Crisis Management Policy of the Distribution System Operator.** Supporting the management of an emergency situation	

4.5.2 Additional national measures for transmission system operators for each crisis scenario

Scenario	Existing measures	
	Preventive measures	**Crisis management measures**
1Cyber-attacks against the critical information technology infrastructure of a system operator and the key system user (TSO's; DSO's; power plants and large industrial customers)	**The scenario should reasonably be divided into two parts.** In the first part of the scenario, the system attack possibilities to be considered must include those that **do not affect the systems directly performing plant control (SCADA)**, but adversely impact the operation of their backend/server systems (e.g. data service systems) or the data stored in them (mainly their integrity and availability, with lower priority on data confidentiality). In the second part of the scenario, the possibility of cyber-attacks against **systems intrinsically linked to the plant control activity (SCADA)** must be analysed. For the systems named in the **first part of the scenario** , it is **possible to launch a (distributed) Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack,** which may make certain ICT systems of the TSO that are important for the regular functioning of the electricity system and the electricity market, inaccessible and	**In order to fend off against such attacks, the TSO will use appropriate security measures as a service,** but it is important to note that these systems primarily serve market activities, the failure of which does not yet pose an immediate threat to electricity supply. The defence for attacks against the SCADA systems linked to the system operation is ensured by the OSP and ISP.

	unusable. Other **attempts at unauthorised access attacks** against the systems identified in the first part of the scenario will be countered by the TSO through a system of protection measures, including **both technical protection solutions and active cybersecurity methods and practices (regular vulnerability scans and penetration testing and hardening).** These technical controls and active cybersecurity activities include **preventive** detective and incident investigation/response (reactive) controls. The **mutual sharing** of **relevant** information (on threats and security events and incidents) among the TSO's cybersecurity protection activities **in a closed circle**, in particular with cyber security experts from European system operators, is of particular importance, as these resources can provide a wealth of information that will allow for faster and more effective action in the event of a wider cyber-attack (against all or part of the European electricity system). The systems identified in the **second part of the scenario** (the unavailability or unauthorised, malicious use of which already **directly threatens the electricity supply**). In such a case, **the TSO must establish a security control environment for such systems within the time limits provided for in the legislation.** For the operational management system, a **tiered border protection system** is already in place to ensure that only authorised users have access to the system resources. A separate control will be included to ensure two-factor identification.	
2 Physical attack on critical assets/equipment	The transmission system operator shall operate **a 24-hour supervised electronic access, intrusion detection and camera system** at all its sites (whether international, national, vital or non-vital) in order to ensure the continuous protection of the facilities and critical equipment at the sites. **The description of the detection**	It is included in the OSP and in the internal Business Continuity Plan.

	and investigation of physical attacks is provided in internal regulations. An appropriate **intrusion detection system** shall be in place to detect a physical attack as soon as possible. This allows unauthorised transactions to be detected through the interface. The protection systems are multi-zone; such protections are designed according to the principle of risk balancing. In the event of an incident, the **critical assets** of the transmission system operator are **built in with redundancy** to reduce the impact. The loss of a certain number of elements of the transmission network may not pose a business continuity risk under the **n-1 principle**. In order to **protect critical assets physically**, the transmission system operator shall design its physical protection systems according to a **security concept** based on uniform principles. Their maintenance and development are planned in advance in line with this objective. The objectives shall be **reviewed annually.** In order to protect critical assets physically, the transmission system operator must apply an **authorisation management system** so that only authorised persons have access to the assets.	
3 Physical attack on the control centre	In order to reduce the likelihood of physical attacks against the dispatch centre(s), the transmission system operator shall operate an **electronic access, intrusion detection and camera system with 24-hour on-site supervision.** With the help of these tools, and with the help of **live service personnel on the site**, physical attacks can be detected early and effectively and thus prevented. The **procedures for the security service** in the event of an **attack on the dispatch centre**, bomb threats and abandoned bags and packages have been specified. In order for the TSO to reduce the risk that a potential guest may	Internal procedures.

	pose a threat to system control, **an internal policy** has been established to establish the **conditions for access to and presence in the control room**. Guests may not enter the premises of the transmission system operator independently; they may only move and stay there under constant supervision.	
4 Hostage taking/threatening/blackmailing of senior personnel	In connection with extortion and threatening and fraudulent e-mails and phone calls, the transmission system operator shall **regularly send out central communication and circulars** to its employees to sensitise them to paying attention to incoming e-mails and phone calls, and to careful consideration of who and what they reply to and what information they send or give. The transmission system operator regularly **reminds its employees** not to click on links in suspicious-looking emails or to provide information about themselves or the transmission system operator on linked websites. Employees are regularly reminded to report suspicious mail to the IT Security Department or the **Information Security Supervisor**, and suspicious phone calls to the **Security Directorate**. The information security readiness of employees is regularly measured by the TSO using **vulnerability testing** and social engineering methods. The transmission system operator operates a spam filter, so there is a kind of filtering for mail generated by machines for fraud and blackmail. Due to the **low risk of extortion and hostage-taking**, **there is currently no specific protocol for this**, but liaison with the authorities is ongoing and an **exercise involving special units** was carried out last year. The transmission system operator's internal regulations must contain a detailed protocol in the event of a terrorist attack in order to minimise the risks involved. In relation to **postings abroad**, the transmission system operator regularly draws the attention of its employees to	It is included in the internal regulations.

	the security-related regulations and warnings specified for the given country on the website of the consular service. The transmission system operator shall also **inform outgoing passengers** individually of the risks in the countries of destination. In the event of a significant security risk, business travel to the particular country shall be prohibited.	
5 Insider attack	In order to **protect business secrets**, the transmission system operator shall sign a **confidentiality statement with all its employees and external partners**, which legally prevents the disclosure of information to third parties. In the case of classified employees, the Transmission System Operator will conduct data reconciliation to ensure compliance with **conflict of interest rules** and will assist **senior staff** in the case of **national security audits** conducted by the competent public authorities as provided for by law. These measures shall reduce the screening of persons who do not comply with the legal and ethical requirements of the transmission system operator upon admission. The transmission system operator operates an authorisation management system to ensure that employees have only the rights they need. Such rights may be physical - the right to access premises, in terms of IT considerations - access to applications and folders. In all cases, the **approval of authorisations is based on the four eyes principle**, on the one hand the approval of the applicant's line manager and on the other hand the approval of the person responsible for the authorisation applied for. Based on the above, employees only have the information and data that are absolutely necessary for their tasks. These authorisations are constantly reviewed during audits. The transmission system operator shall pay particular attention to minimising the adverse effects of a possible	It is included in the internal regulations.

	event. Any **violation of physical access rights** (e.g. someone trying to enter a room to which they have no right) is immediately **detected by the 24-hour security service on duty on site**, **according to the procedural protocol laid down in the local security guarding instructions.** **IT sabotage is prevented by a 24-hour NOC (Network Operations Centre).** Major IT incidents are investigated in all cases, also from the point of view of excluding the possibility of intentional sabotage, including internal sabotage.	
6 Storm	The transmission system operator shall, as a principle, protect itself against the risks arising from extreme weather events (regardless of their nature) by ensuring **adequate sizing during the establishment of the network**. The **newly established transmission lines will be constructed in accordance with level 1** (a weather condition that takes place once every 50 years) **according to the MSZ EN 50341 standard**. In **critical high-priority locations** (motorways, trunk roads, railways, rivers and border crossings), **transmission lines are installed according to the standard level 2** (weather phenomenon occurring every 150 years). The conversion of the network transmission lines of the South Pest region to level 2 is in progress. Based on the technical specifications of the **equipment of the transmission network substations** (bus bar, shunt choke, circuit breaker, measuring transducer, disconnector, transformer, and surge arrester), it can be said that **they can withstand a load corresponding to a wind pressure of at least 700 Pa.** In addition to sizing, in order to prepare for ad hic extreme weather conditions, certain **network maintenance works may be postponed or rescheduled if justified on the basis of weather forecast data.** The **transmission system**	The transmission system operator shall **operate a standby system that provides on-site arrival within 1 hour of the alarm for substations and within 2 hours for transmission lines.** The transmission system operator **has several provisional poles for 220 and 400 kV transmission lines for the temporary replacement of damaged transmission line poles**, which can be installed in a few days if necessary, and **has the necessary materials for transmission line construction**, so the restoration can start immediately (before the lengthy procurement procedure). In addition, the transmission system operator has an **on-call contract to deal with substation, transmission line, control and communications failures.** If **the absence of network elements lost due to extreme weather causes a network bottleneck**, the transmission system operator shall **select the most appropriate one (from a technical and economic point of view) of the intervention measures available to it.** First of all, preference must be given to **measures and topological interventions that do not entail costs.** However, if the bottleneck cannot be eliminated through network topology measures, the transmission system operator shall make interventions that **entail costs and may include internal or**

	operator receives a 3-day forecast from the National Meteorological Service (OMSZ) **on a daily basis**, and the system operator and work managing dispatchers have **access to the OMSZ meteorological information system showing the current weather conditions.** If a **transmission network element (e.g. transmission line) is damaged** by extreme strong winds and/or extraordinary load due to hoarfrost, the recovery of the lost element must be started as soon as possible.	**cross-border redispatching or multilateral remedial action (MRA).** As an **ultimate action**, if the bottleneck cannot be eliminated by other means, the transmission system operator may **impose (local) restrictions on consumers.**
7Heavy rainfall and flooding	**Since it is a natural phenomenon**, the transmission system operator has no control over heavy rainfall events, including the floods they cause, and therefore cannot specify risk mitigation measures. Based on the geographical conditions of Hungary and the available historical data, **this risk is managed** by the transmission system operator **with a low probability of occurrence**, because the probability of a flood with a dangerous outcome for the Company is low. Due to the location of the transmission system operator's **headquarters**, it can be concluded that it is not located in an area at risk of flooding or inland flooding. **With regard to the headquarters, there is a risk of sudden flooding**, however, based on the previously mentioned data; this risk is identified by the transmission system operator **with a low probability of occurrence**. Despite the low risk classification, **a flood plan has been developed in the** transmission system operator's **internal regulations.** The **regulations set out the preparatory tasks** for the reduction of damage caused by floods, and the **actions to be taken** in the event of a flood and after the flood. In relation to the elements of the transmission network, in order to reduce the impact in the event of heavy rain and	In order to **mitigate the consequences of a possible sudden flood**, the transmission system operator shall operate a **back-up facility** providing full functionality for which no such risk has been identified. In-house action plan.

	floods, the **critical assets** of the transmission system operator **have been redundantly deployed.** The loss of a certain number of elements of the transmission network may not pose a business continuity risk under the **n-1 principle**.	
8 Extreme winter weather event	The transmission system operator shall, as a principle, protect itself against the risks arising from extreme weather events (regardless of their nature) by ensuring **adequate sizing during the establishment of the network**. The **newly established transmission lines will be constructed in accordance with level 1** (a weather condition that takes place once every 50 years) **according to the MSZ EN 50341 standard**. In **critical high-priority locations** (motorways, trunk roads, railways, rivers and border crossings), **transmission lines are installed according to the standard level 2** (once every 150 years). **Reconstruction of the pipelines established in accordance with the previous MSZ 151 standard is taking place in the case of the transmission line, which has been considered critical by the transmission system operator.** Based on the technical specifications of the **equipment of the transmission network substations** (bus bar, shunt choke, circuit breaker, measuring transducer, disconnector, transformer, and surge arrester), it can be said that **they can withstand a load corresponding to a wind pressure of at least 700 Pa.** In addition to sizing, in order to prepare for eventual extreme weather conditions, certain **network maintenance works may be postponed or rescheduled if justified on the basis of weather forecast data.** The	The transmission system operator shall **operate a standby system that provides on-site arrival within 1 hour of the alarm for substations and within 2 hours for transmission lines.** The transmission system operator **has several provisional poles for 220 and 400 kV transmission lines for the temporary replacement of damaged transmission line poles**, which can be installed in a few days if necessary, and **has the necessary materials for transmission line construction**, so that restoration can start immediately (before the lengthy procurement procedure). In addition, the transmission system operator has an **on-call contract to deal with substation, transmission line, control and communications failures.** If **the absence of network elements lost due to extreme weather causes a network bottleneck**, the transmission system operator shall **select the most appropriate one (from a technical and economic point of view) of the intervention measures available to it.** First of all, preference must be given to **measures and topological interventions that do not entail costs.** However, if the bottleneck cannot be eliminated through network topology measures, the transmission system operator will make interventions, which **entail costs and may include internal or cross-border redispatching or multilateral remedial action (MRA).** As an **ultimate action**, if the bottleneck cannot be eliminated by other means, the transmission system operator may **impose (local) restrictions on consumers.**

	transmission system operator receives a 3-day forecast from the National Meteorological Service (OMSZ) **on a daily basis**, and the system operator and work managing dispatchers have **access to the OMSZ meteorological information system showing the current weather conditions.**	
9 Fossil fuel shortages (including natural gas shortages)	The lack of fossil fuels in Hungary can basically be divided into two main directions due to the peculiarities of the Hungarian power plant fleet. On the one hand, it may be encountered in the case of the Mátra Power Plant, due to **interruptions in the supply of lignite**, and on the other hand, it may arise in relation to the supply of our **natural gas-fired power plants**. The **lignite-fuelled** units of the Mátra Power Plant do not have an alternative fuel supply but, due to the local conditions and the availability of primary energy carriers in the vicinity, there is no need to fear major and lasting risks, and **any shortage of lignite supply is limited to weather conditions, which are the responsibility of the power plant and mining industry.** As the **supply of fuel to natural gas-fired power plants is vital** for the safe operation of the domestic electricity system and the supply of district heating to many districts, **a number of measures and statutory provisions have been adopted to facilitate it**: • **Natural gas-fired power plants have been classified into natural gas control categories**, and consequently, according to the principles set out therein, it is necessary to provide them with a fuel supply. In practice, this means that, in the event of natural gas supply problems, these power plants take precedence over access to fuel.	In the event of a **persistent fuel shortage**, ordering interventions that directly affect consumers in order to maintain the safe operation of the electricity grid may be unavoidable. **This is achieved by imposing restrictions on consumers and applying a** Rotating Load Shedding System**.** As a further solution, the **application of the provisions of the international cooperation agreements** currently in force may arise.

	• A **significant part of the natural gas-fuelled power plants** (Gönyű, BERT, Csepel, Dunamenti G2, and Bakony GT) **have alternative fuel reserves, as they can also operate using fuel oil. This obligation is laid down in GKM Decree No. 44/2002. (XII. 28.).** If necessary, in particular in preparation for the winter period or in the event of any circumstances that could threaten regular operations, such as a pandemic, the transmission system operator shall **collect information from market partners on available alternative fuel supplies and their replenishment, and conduct compliance checks under different shortage scenarios.**	
10 Loss of critical information and communication technology infrastructure required for real-time or near real-time electricity system management	The most critical IT systems used for system management are the plant management systems, for which protection against "the failure of information and communication technology infrastructure" has been designed according to the principle of protection proportionate to the risks. In the case of an operations management system, a **robust design that can withstand multiple failures** is a given at all levels of the infrastructure, including duplication of major server functions within the system (live and standby). **Redundancy is also built into the telecommunication lines, which include geographically divergent paths.** **The network and network security infrastructures** serving the systems **are also built with built-in (both on-site and geographically separated) redundancy.**	Transition to reserve systems based on internal regulations and action plan.

11 Unplanned flows due to physical flows that do not follow market-scheduled flows	With an uncoordinated, **NTC-based capacity calculation mechanism** based on **individual modelling, market schedules can deviate significantly** from the actual physical flows at the bidding zone boundaries. Recognising this risk, coordinated **system security cooperations** have been developed in Europe to predict real power flows accurately in the operational planning (day-ahead and intraday) timeframe, based on market schedules and network models. **Coordinated operational security analyses** enable actual physical flows to be modelled more accurately, so that system operators can prepare for real power flows during the operational planning phase by taking intervention measures (at no or low cost) if necessary. The **contingency analysis conducted during coordinated operational security tests** provides an opportunity to comply with the N-1 safety standard. The shift from NTC-based to flow-based capacity calculation mechanisms for short-term (day-ahead and intraday) capacity allocation, as required by the Capacity Allocation and Congestion Management guideline (CACM), represents a further step forward in mitigating the risks arising from differences in schedules and physical flows. Indeed, the main objective of a flow-based capacity calculation mechanism (ensuring maximum capacity release, while ensuring transparency and non-discrimination) is to bring trade and physical reality closer together.	If the transmission system operator detects network bottlenecks during operational safety inspections (i.e. overload or non-standard voltage or their risk) it shall choose the most appropriate **intervention measures** (from a technical and economic point of view) from among those available to it. First of all, preference must be given to **measures and topological interventions that do not entail costs.** However, if the bottleneck cannot be eliminated through network topology measures, the transmission system operator shall make interventions, which **entail costs and may include internal or cross-border redispatching or multilateral remedial action (MRA).** As an **ultimate action**, if the bottleneck cannot be eliminated by other means, the transmission system operator may **impose (local) restrictions on consumers.**
12 A significant industrial or nuclear accident with prolonged nuclear or toxicological contamination, which may	Preventive action is not available to the TSO; it cannot influence the prevention of a possible crisis.	In the event of a nuclear disaster, the **Government of Hungary must take immediate action and declare a state of national crisis.**

result in long-term loss of personnel (months or years)		The Transmission System Operator **can avoid or mitigate customer curtailment and ensure uninterrupted electricity supply,** which is, of course, essential for the rapid resolution of a crisis, **by using** its knowledge of the grid conditions, **electricity import options, available generation capacity and international cooperation.**
13 Out-of-specification estimation error in renewable energy generation	Due to the growing share of renewable producers, it is becoming increasingly important to improve their scheduling accuracy, and for this reason, (through financial means) market participants must be encouraged to do so. **Article 5 of Regulation (EU) 2019/943 on the Internal Market in Electricity, which stipulates that "all market participants must be liable for any imbalances they cause in the system"** is intended to serve this purpose. According to the regulation, from the business month of April 2020, **the cost of balancing energy of the Compulsory Power Purchase Balancing Group will be reallocated to the members of the Compulsory Power Purchase Balancing Group causing the imbalance**, and the related costs will be borne by the members, i.e. it is in the economic interest of market participants to report schedules as accurately as possible. It is important to note, however that, in accordance with Government Decree No. 389/2007. (XII. 23.) on the Compulsory Purchase and Purchase Price of Electricity Generated from Renewable Energy Sources or Waste Energy and Cogenerated Electricity (Compulsory Power Purchase Decree) and Government Regulation No. 299/2017. (X. 17) on Mandatory Purchase and Premium Support for Electricity Produced from Renewable Energy Sources (METÁR Decree), the electricity produced from renewable energy sources and waste energy is not subject to the same conditions as electricity produced from waste energy; **the cost of balancing energy is only partially borne, as market operators are compensated. The level of**	If the system's reserves are still exhausted, the transmission system operator **may request international assistance and, as a last resort, impose restrictions on consumers**.

	compensation will decrease each year, reaching zero in 2026. The scheduling accuracy of generators of electricity from renewable resources is, of course, limited by the reliability of the meteorological forecast, but there are **several tools available to market participants to improve the accuracy of the data provided.** On the one hand, **all data submitters have the possibility to modify the schedulewithin the day, thus clarifying the schedule submitted the day before with an H-2 hour lead time (expected to decrease further).** On the other hand, the **producer subject to the Compulsory Power Purchase Decree has the opportunity to join a Scheduling Group Representative (Aggregator or SGR)**, so the SGR provides the data instead and bears the resulting sanctions (regulatory surcharge). The main advantage of this option is the portfolio effect, as the even distribution of the different production units over a large geographical area allows a much more accurate estimation, due to the independence of the production run from local weather factors, and the sharing of the cost of purchasing meteorological forecast data from different providers also demonstrates the economic rationality of clustering. It is important to emphasize that **imbalances due to scheduling inaccuracies of renewable generators must be taken into account in the reserve sizing mechanism applied by the transmission system operator.** The likelihood that the reserve capacities committed by the transmission system operator will not cover the imbalances of renewable producers (due to an estimation error) is negligible.	
14 Pandemic	The pandemic is a health and social issue, and therefore **no effective action can be taken by the transmission system**	Based on the in-house action plan.

	operator to prevent it from happening. In relation to the pandemic, **it can only take measures to mitigate the resulting impact** on the transmission system operator. In this regard, it continuously **reviews and updates its internal regulations.** In addition, in order to reduce the direct impact on the transmission system operator, a **Pandemic Committee shall be formed** from the managers (headed by the Security Director), which will **meet** weekly or **even daily**, depending on the situation, and take **effective measures** to assess and examine the circumstances and impacts. in order to ensure the continuity of business continuity at all times. The most important measures to be taken by the transmission system operator in the event of a pandemic include the following: • Provision of continuous medical check-ups for employees. • Provide flu vaccination for employees. • Provide testing for employees (where technologically feasible). Regular testing is mandatory for critical staff. • Significant restrictions on access to the headquarters - dispatch centre and the backup site. In all cases, access by external employees is subject to the permission of the Security Directorate. • Continuous provision of protective equipment for employees. Increase in the number of cleanings (for disinfection). • Depending on the symptoms of the infection, the performance of non-contact body temperature measurement at the headquarters and at the backup site, if relevant	Following the introduction of restrictions, departments must keep the timetable of ongoing and planned projects and developments under review and check whether and how deadlines are affected.

	• If necessary, creation of the conditions for the migration of critical staff for a certain period of time. • Providing travel between work and residence without the use of public transport. • Ordering continuous home office work for employees whose work does not require a stay at headquarters, providing the conditions for this. • Regular corporate communication for employees. • Establishment of permanent teams for multi-person services (to reduce contact numbers) • Sharing information by telephone instead of handing over and receiving personal services The decisions of the transmission system operator are largely determined by the measures taken by the Government of Hungary, such as the introduction of qualified periods - state of national crisis, state of emergency, and state of danger.	
15 Heatwave	As a result of climate change, the impact of prolonged hot summer weather and heat waves on the electricity system is expected to become increasingly significant, as evidenced by trends in recent years. The photovoltaic capacities rapidly expanding in Hungary are only able to compensate for this effect to a limited extent. **Environmental regulations** impose strict requirements on power plants, with river water mixed with cooling water flowing back into the river not exceeding certain temperatures. During prolonged droughts and heatwaves,	The main options available to the transmission system operator to make up for the lack of generating capacity and electricity due to heatwave and drought are the use of **system-level services, the use of available regulation capacity,** and in extreme cases**, redispatching,** or international relief. If these are exhausted, it may be necessary to impose restrictions on consumers, or to apply the Rotating Load Shedding System.

	the water flow of the Danube decreases significantly and its water temperature rises. In such cases, the transmission system operator has to consider the **generation output reduction obligations of the Paks Nuclear Power Plant,** the coercive nature of which has been on the agenda over the last decade, during longer hot summer periods.	
16 Dry period	As a result of climate change, the impact of prolonged hot summer weather and heat waves on the electricity system is expected to become increasingly significant, as evidenced by trends in recent years. The photovoltaic capacities rapidly expanding in Hungary are only able to compensate for this effect to a limited extent. **Environmental regulations** impose strict requirements on power plants, with river water mixed with cooling water flowing back into the river not exceeding certain temperatures. During prolonged droughts and heatwaves, the water flow of the Danube decreases significantly and its water temperature rises. In such cases, the transmission system operator has to consider the **generation output reduction obligations of the Paks Nuclear Power Plant,** the coercive nature of which has been on the agenda over the last decade, during longer hot summer periods.	The main options available to the Transmission System Operator to make up for the absence of generating capacity and electricity due to heat wave and drought include **the use of system-level services, the use of available regulation capacity**, and in extreme cases, **redispatching, or international relief.** If these are exhausted, it may be necessary to impose restrictions on consumers, or to apply the Rotating Load Shedding System.
17 Earthquake	Due to natural effects, the transmission system operator has no control over earthquakes and therefore cannot set mitigation measures but, based on the geographical characteristics of Hungary and the available historical data, it treats this as a low probability risk, because the probability of an earthquake with a dangerous outcome for the transmission system operator is low. Nevertheless, an action plan has been developed in **internal regulations in the case of earthquakes**, and in order to maintain business continuity, **work at the reserve**	Moving to a reserve site according to the internal rules.

	site is ensured if, due to an earthquake, it is impossible to operate at the original site. In the event of an earthquake, the critical assets of the transmission system operator are **redundantly installed to reduce the impact.** The loss of a certain number of elements of the transmission network should not pose a business continuity risk under the **n-1 principle**.	
18 Wildfire	**There is no regulation/standard to be taken into account** for the construction of substations **due to the risk of wildfires, since it is considered as an emergency.** The transmission system operator **prevents the growth of vegetation in the openings of the built transmission lines by regular maintenance (twig removal).** In order to provide effective and rapid protection against fires, the transmission system operator must **liaise with the local fire service, which shall conduct regular fire-fighting exercises at the transmission system operator's substations.**	The transmission system operator shall **operate a standby system that provides on-site arrival within 1 hour of the alarm for substations and within 2 hours for transmission lines.** The transmission system operator **has several provisional poles for 220 and 400 kV transmission lines for the temporary replacement of damaged transmission line poles**, which can be installed in a few days if necessary, and **has the necessary materials for transmission line construction**, so that restoration can start immediately (before the lengthy procurement procedure).

4.5.3 Additional national measures for large power plants for each crisis scenario

Scenario	**Existing measures**	
	Preventive measures	**Crisis management measures**
1 Cyber-attacks against the critical information technology infrastructure of a system operator and the key system user (TSO's; DSO's; power plants and large industrial customers)	Operating appropriate security measures: - firewall, - separation of industrial and office networks, - minimising the Internet connection of industrial networks	System recovery based on continuous system backups. (Based on the relevant plans.)

2 Physical attack on critical assets/equipment	Adequate level of guard protection (technology and manpower),	Adequate alarm system (police, ambulance, disaster management, fire service)
3 Physical attack on the control centre	Establishment and maintenance of an alternative (backup) control centre. Operation of access control system (s) subject to authorisation and identification.	
4 Hostage taking/threatening/blackmailing senior personnel	Sharing tasks and responsibilities, and making information widely available.	
5 Insider attack	-	-
6 Storm	-	-
7Heavy rainfall and flooding	Design and construction appropriate to the prevailing climatic conditions.	To be determined on a case-by-case basis.
8 Extreme winter weather event	Preparing equipment for operation in expected extreme winter weather conditions.	
9 Fossil fuel shortages (including natural gas shortages)	Oil stockpiling according to the decree, maintenance and upkeep of oil technology, regular operational tests, and the maintenance of a fuel contract.	Commercial risk management, reduction of scheduled generation (coverage) in potential periods affected by natural gas shortages. Alternative fuel operation.
10 Loss of critical information and communication technology infrastructure required for real-time or near real-time electricity system management	-	-
11 Unplanned flows due to physical flows that do not follow market-scheduled flows	-	-
12 A significant industrial or nuclear accident with prolonged nuclear or toxicological	Develop and practice emergency scenarios from time to time at the appropriate level so that staff are aware of	Based on the in-house action plan.

contamination, which may result in long-term loss of personnel (months or years)	what to do, in order to minimise downtime and being affected.	
13 Out-of-specification estimation error in renewable energy generation	-	-
14 Pandemic	Minimise the number of contacts by (re)organising work schedules. Design and operation of system for the provision of personal protective equipment that provides adequate protection. The operation of a testing system to establish the presence of infection.	Introduction and operation of alternative work schedules.
15 Heatwave	Preparing equipment for operation in expected heatwave and extreme hot weather conditions.	
16 Dry period	*Hydroinfo* Danube water level 5-day forecast continuous processing, development of an operational readiness system depending on the expected Danube water level – where relevant. Preparing for water extraction with adequate safety during low water periods by installing flexible water abstraction structures and devices.	To be determined on a case-by-case basis.
17 Earthquake	Design and construction in accordance with the typical seismic conditions, preservation of facilities.	To be determined on a case-by-case basis.
18 Wildfire	-	-

4.6 Public information measures in the event of an electricity supply crisis

Public information at national level is provided by the transmission system operator's communication department, with the involvement of the communication officers in the information system (including the competent authorities designated under the risk preparedness regulation), through the printed press and electronic media, on the basis of internal instructions from the transmission system operator.

Organisations included in the information system:

a) State organisations: Ministry of Innovation and Technology, Ministry of Agriculture, Hungarian Energy and Public Utility Regulatory Authority, Disaster Control Directorate of the Ministry of the Interior, county disaster control directorates,

b) System users: dispatcher services of distribution network licence holders, dispatcher services of generation licence holders, national dispatcher service of the transmission system operator, transmission directorate of the transmission system operator and regional operational centres (ROCs), traders conducting more than 5% of the electricity industry turnover, universal service providers.

The transmission system operator may, in addition to providing appropriate information through the media, request users to reduce the user load voluntarily:

- in the event of a significant disturbance, long-term significant disturbance and network disturbance specified in the Government Decree and the Operating Regulations;
- the risk of a level I or level II crisis situation as defined in the Government Decree;
- on the instructions of the Government in a crisis situation;
- in the event of other systemic malfunctions, as defined in the Operating Rules, which do not result in significant disruption and which may require the imposition of user restrictions.

In the event of a foreseeable crisis, a notice of possible user outages must be issued at least 48 hours in advance of the outages and immediately in the case of a foreseeable crisis 24 hours or less.

During the crisis, the transmission system operator shall issue new notices on events and interventions in the electricity system with modified content and publication conditions.

If it becomes possible to withdraw user disconnections, the transmission system operator shall issue a notice to that effect and, if possible, withdraw its request for voluntary load shedding.

Communications on the crisis will be sent (in writing) by the transmission system operator's communications department to the communications officers of the other electricity companies concerned simultaneously with dispatching them to the public media service providers, in order to ensure coordinated information.

Public information at the local level is provided by the communication staff of the licence holders in accordance with their own internal regulated procedures and under their own authority.

To inform society through the media, it is necessary to publish coherent and interlinked information. The best way to provide for this is to ensure that the staff who compile the messages have access to the information relevant to their area as soon as possible, i.e. that the communication officer of the issuing organisation sends it to the other stakeholders at the same time as it is sent to the media.

The list of relevant staff and their contact details must be kept up to date to ensure communication between the communication officers. Changes must be reported to the communications department of the TSO, which shall ensure that the list is kept up to date.

4.7 Regional and bilateral procedures and measures

4.7.1 Mechanisms adopted to ensure intra-regional cooperation and appropriate coordination before and during the electricity supply crisis, including decision-making procedures to ensure an appropriate response at regional level

EAS (ENTSO-E wide awareness system)

The EAS is a SCADA system that displays system-level status based on real-time data received from all ENTSO-E member TSOs via the Electronic Highway, which is available to all TSOs. The scope of the information provides an overview of system-wide cooperation and quick detection of possible malfunctions, using user-friendly graphical images.

Main functions:

- system status display showing the current status of each TSO (regular, alarm, emergency, blackout and system recovery)
- the frequency of TSOs in the synchronous zones, detecting possible system breakdown and identifying islands
- power balances in regulatory zones and instantaneous values of cross-border flows, export-import balances
- type distribution of producers by regulatory zone
- user adjustable trend data display
- measurement archive for ex-post analysis
- a "message board" to replace telephone communication and facilitate the flow of information in the event of a system failure, through which any or all TSOs can be contacted.
- display of important parameters of the islands in case of system failure (status of controllers, display of the TSO performing frequency regulation, display of the TSO performing re-synchronisation)

The EAS system is operated by RTE and Amprion, in parallel mode (multisite system), so the failure of either side does not cause any loss of information. Tests are carried out on a quarterly basis with all TSOs to verify reliable operation.

Operational procedure for critical grid situations (CGS):

A Critical Grid Situation (CGS) is a potential emergency condition that is identified during the preparation for operation and occurs when the normal preventive measures (PST grade control, topological interventions, internal, bilateral or multilateral re-dispatch) have been exhausted and have not yielded satisfactory results. As a result, TSOs will need to implement regionally coordinated measures.

A CGS, as a process of regionally coordinated emergency interventions, will be implemented in the TSC region as one of the last measures to prevent serious disruptions associated with system failure. Current DACF and IDCF processes are not designed to address these critical situations as they are preceded by an inadequately coordinated capacity calculation process. The time window is too narrow for the DACF or IDCF process to offer a meaningful solution to such situations, so the CGS process extends the handling of critical situations to time periods D-2 and D-3.

The identification of the CGS should be based on the results of load-flow calculations for critical network elements, which are derived from the forecast market results. This will require the creation of the Early Load Flow Forecast (ELFF) as a new RSC process that is part of the Early Warning Process. The next step is to check the extent to which the standard intervention options provide a solution to the bottleneck problem. If there is a possibility of overload even if these interventions are exhausted then emergency measures will be required, which may include:

- Additional re-dispatch: there are units suitable for redispatch with a start-up time of more than 12 hours. These units must be taken into account in critical situations detected during the time periods D-3, D-2, and D-1.
- Modification of day-ahead cross-border capacities: this part of the CGS process is applicable for the D-2 time period, but only if the available re-dispatch options are not sufficient to reduce bottlenecks.
- Limitation of reserved cross-border capacities: if capacity modifications are not sufficient to deal with bottlenecks, capacity limitations may be necessary. As with the amendment, the restriction will be applied over a period of D-2, based on the same methodology (boundary section, direction, volume determination).

STA process – Short-term adequacy process:

According to Article 81 of the SO GL and Article 9 of Regulation (EU) 941/2019 of the European Parliament and of the Council on electricity sector risk preparedness, Regional Security Coordinators (RSCs) (from 01.07.2022 Regional Coordination Centres (RCCs)) carry out Short Term Adequacy (STA) assessments.

The STA Operational Safety Service is a Europe-wide performance compliance test. It aims to identify any foreseeable capacity gaps within a one-week timeframe, based on the available generating capacity in each country, the available interconnection capacity and the expected user demand. From the input data provided by the TSOs, a cross-regional STA analysis is performed on a daily basis, showing the risk of deficits, taking into account the uncertainty of renewable production, the impact of different weather conditions on consumer needs and the probability of producer and network outages. To address the shortage identified in the analysis within the next three days, the TSOs concerned, under the guidance of the RSC(s), shall propose coordinated preventive intervention measures along the established process of the regional STA process.

ITA – Inter TSO agreements:

International Operational Agreements (ITAs) establish the legal and technical framework for network operation and system operation between neighbouring TSOs. MAVIR has such an agreement with all neighbouring TSOs with which it has a jointly operated and operated cross-border transmission line (APG, SEPS, Ukrenergo, Transelectrica, EMS, HOPS). A similar agreement is being prepared with the Slovenian system operator (ELES) for when the Hungarian-Slovenian cross-border transmission line will be operational.

The above-mentioned agreements of MAVIR have a similar structure, modelled on the agreements concluded by Western European TSOs. The body text sets out the legal framework for cooperation between TSOs, also referring to the international standards under which TSOs must carry out their tasks. It also reviews the areas of expertise and the main principles of cooperation related to them, in which cooperation or information sharing between the two TSOs is required. The specific technical and other details according to the topic are typically contained in 18-20 annexes. The agreements are structured in such a way that any technical, methodological or procedural changes in the cooperation can be managed by the TSOs by updating the relevant annex(es) - without changing the body text.

The annexes also contain the measures to be taken by the TSOs in order to maintain operational safety and in the event of a breakdown and system recovery. With regard to operational safety, the aim is to maintain the (n-1) principle applied in the operation of the electricity system (to restore it in the event of a breakdown). The agreements do not cover measures to be taken in extreme situations beyond the realistic possible disturbances in the operation of the electricity system.

Participation in TSCNET:

The main task of TSC cooperation is to perform coordinated operational safety calculations in a pan-European grid model (CGM) and to coordinate the necessary intervention measures between TSOs. TSCNET acts as a coordinator to facilitate the work of the members involved in the collaboration. It operates the safety investigation platform (AMICA) and manages the calculation processes. The calculation processes basically involve forward-looking load-flow and contingency analysis, which accompanies the plant from D-1 to the actual operating state. It consists of three main processes:

- DACF – Day-Ahead Congestion Forecast
- IDCF – Intra-Day Congestion Forecast
- RTSN – Real-Time Snapshot

The difference between these processes is the time lag compared to the time reviewed, as a result the input data (outages, schedules) become closer and closer to the real operating state to the examined time as time progresses.

During the DACF process, the network calculation tool determines the expected flow pattern for the next day, depending on the planned outages and schedules, for the 30th minute of each hour. To do this, each TSO first generates its own grid model (IGM), which includes scheduled outages for the next day and power plant and export-import schedules, and then combines these models to create a common grid model (CGM) on which a load-flow and contingency analysis is run. From the results of the load-flow and contingency analysis, it can be read whether a network bottleneck is expected or whether a downtime could endanger operational safety. In each case, the process continues with a video conference (DOPT), where each TSO can share whether it has detected any bottlenecks in its territory and what intervention measures can be taken to eliminate the bottleneck, even with the help of other TSOs (network interventions, re-dispatch and MRA).

The IDCF process starts on day D, which is a rolling process that checks the remaining hours of the day; the process is the same as the DACF process, but includes possible intra-day schedule changes, and the network model is more accurate, as it includes unforeseen outages/outages on day D-1. This results in more accurate load-flow and contingency analysis results for the actual operating condition. During the IDCF process, a video conference (IDOPT) will only take place if the resulting bottleneck can only be resolved with the help of the other TSOs.

The RTSN process is the calculation that most accurately predicts the real-time operating status of the processes operated by TSCNET; here the model service and the calculation take place every 15 minutes. Its purpose is not to serve operational plant management, but to control the quality of models sent over longer periods of time.

The primary goal of the coordinated operational safety investigations is to support the operational operation management, to detect any foreseeable network bottlenecks, and to search for and validate the intervention measures necessary for their resolution. This will mainly reduce the likelihood of critical operating conditions due to network outages, expected consumer (extreme load conditions caused by weather conditions) and generation conditions (extreme operating conditions caused mainly by increasing renewable generation) and insufficiently coordinated transmission network outages (at TSO level).

MRA contract:

The Multilateral Remedial Action (MRA) process is part of the TSO Security Cooperation (TSC), a contractually regulated operational security process involving the majority of TSC member TSOs, in which MAVIR has been participating since 2015. Its aim is to enable system operators to manage unplanned flows and bottlenecks in the Central European region, which threaten operational safety, even if their own resources or bilateral interventions are no longer sufficient or are technically inefficient. The system operators participating in the MRA then have the opportunity to use the intervention options available in the region to remove bottlenecks, under central coordination and through a unified process.

Since the process typically involves power plant redispatch, the MRA contract also includes a cost-sharing policy for this.

International assistance agreements:

In order to prevent large-scale system malfunctions, MAVIR has concluded international emergency assistance contracts with several (primarily neighbouring) system operators, the basic purpose of which is to prevent the harmful effects of power shortages and to manage network bottlenecks. Large power imbalances can cause the steady-state frequency deviation to exceed the standard 50 MHz band due to system imbalance, and the management of network bottlenecks is essential because overloaded elements can cause cascading protection operations, which can lead to the breakdown of the power system.

MAVIR has concluded international emergency assistance with the following system operators:

- HOPS (Croatia)
- PSE (Poland)
- Transelectrica (Romania)
- EMS (Serbia)
- Ukrenergo (Ukraine)
- APG (Austria)

International disaster relief is primarily a bilateral agreement established to address domestic production shortfalls as well as domestic and cross-border bottlenecks. The quantity that can be requested is determined, among other things, by the free network capacity available at the border crossing, as it can be used at its expense, as well as the available free production capacity that the assisting country can provide. All contracts are two-way, so both system operators can be both transmitting and receiving parties. There is no pre-committed border crossing network capacity for backup purposes; it can be provided mainly from the TRM, which is the reliability reserve of the border-crossing, thus trading does not affect its level, only the network environment. If requested, it may be granted in addition to the TRM if there is free border inspection capacity available during the period of the assistance. The available production capacity depends on the current availability of the domestic power plant park (operating status of the power plant units, weather-dependent technical limits), production schedules and the previous day's operational preparation (we do not offer reserved reserve capacity).

The actual usable quantity is clarified within the framework of telephone consultation, and the usage is recorded in writing on a confirmation form (specifying the product period, direction, quantity and in most cases price), which is approved by the service manager of both system operators. The advantage of international assistance is that the contract specifies the time and form of each single step, so that at the critical moment, the operator can take the necessary steps on the basis of precise guidelines, thus facilitating recourse.

Hungary's existing bilateral agreements with neighbouring countries in the electricity sector:

- As regards Romania: *Act LIV of 2010 on the promulgation of the Agreement between the Government of the Republic of Hungary and the Government of Romania on Cooperation in the Field of Natural Gas Transmission Pipelines and Electricity Transmission Lines Crossing the Hungarian-Romanian State Border.*

- As for Croatia: (i) *Act XXXIII of 2010 on the proclamation of the Agreement between the Government of the Republic of Hungary and the Government of the Republic of Croatia on Cooperation in the Construction, Operation, Maintenance, Reconstruction and Emergency Repair of Electricity Transmission Lines Crossing the Common State Border,* and (ii) *Act CXXXVII of 2011 on the Proclamation of the Agreement between the Government of the Republic of Hungary and the Government of the Republic of Croatia on Cooperation in the Field of Increasing the Security of Energy Supply.*

- As for Slovenia: *"Memorandum of Understanding on Cooperation in the field of Energy between the Ministry of Transport, Telecommunication and Energy of Hungary and the Ministry of the Economy of the Republic of Slovenia"*

5 Crisis coordinator

The CC acts as crisis coordinator. In order to prevent and prepare measures in case of an electricity crisis, the TSO operates a CC. The Crisis Working Committee is composed of the chair of the TSO and 8 members - two representatives each from the generation licensees and distributors, the transmission system operator, the nuclear power plant, the universal service providers and the electricity traders. The CC operates as a body with its own rules of procedure, including contact details for its members.

The CC may delegate the role of crisis coordinator to the TSO for the purpose of taking operational management measures requiring immediate intervention in real time and for liaising with the crisis coordination body referred to in Article 12(1)(a) of the Risk Preparedness Regulation, while informing the Agency.

The availability of CC will be added in the final version.

6 Consultations with stakeholders

Further work in progress.

Pursuant to Article 10(1), it describes the schemes used for consulting the parties specified below in order to develop this plan and the results of the consultations:

a) the affected electricity and gas undertakings, including the producers concerned or their professional organisations;

b) stakeholder organisations representing the interests of non-industrial electricity consumers;

c) stakeholder organisations representing the interests of industrial electricity consumers;

d) regulatory authorities,

e) transmission system operators;

f) the distribution system operators concerned.

On 12 March 2021, the Authority conducted a preliminary electronic consultation of the industry licensees involved in the consultation process for the definition of the national crisis scenarios on the national measures required in the risk preparedness plan, in accordance with Article 11(1)(c), (f), (g) and (h) of the Risk Preparedness Regulation.

The Authority has received comments from the TSO, six DSOs and one licensee for large power plants, which were incorporated into Chapter 4.5 of the Risk Preparedness Plan (additional national measures for each crisis scenario).

With regard to the national consultation referred to in Article 10(1) of the Risk Preparedness Regulation on 26 July 2021, the HEA put forward the draft of the Hungarian Electricity Supply Risk Preparedness Plan for industry consultation. The Authority accepted comments and suggestions from industry players and sectoral organisations electronically until 26 August 2021. On the HEA's website, a permanent notice box called the attention of the industry players to the consultation during the reference period.

The link announcing the public consultation:

http://www.mekh.hu/iparagi-konzultacio-a-magyar-villamosenergia-ellatasi-kockazati-keszultsegi-tervrol

Answering the call of the Hungarian Energy and Public Utility Regulatory Authority, four industry players and organisations submitted comments during the reference period.

Therefore, the Risk Preparedness Plan is hereby appended with a description of the industry consultation process, the opinions received, and the manner in which they were taken into account.

The purpose of Annex I. is to describe the opinions received during the consultation and the results of these opinions being taken into consideration by the Authority in detail.

7 Emergency Tests

They are being developed - regional and international consultations are required.

a) Provide a timeline for a two-year regional (and, if available, national) real-time simulation of electricity supply crisis responses;

b) In accordance with Article 12(1)(d), specify the procedures adopted and the actors involved.

To update the plan: briefly describe the tests carried out since the last plan was adopted and their main results. Specify the measures that have been adopted as a result of these tests.

8. Closing remarks

HEA – in consent with the Ministry of Innovation and Technology – will initiate the modification of Government decree 280/2016. (IX. 21.).

The modification will serve the purpose of giving legal mandate to the Crisis Working Committee to execute the role of Crisis Coordinator in accordance with the draft Risk Preparedness Plan and in order to execute all the tasks it is mandated by the draft Risk Preparedness Plan with regards to managing the most relevant national electricity supply crisis scenarios included in Chapter 2. of the draft Risk Preparedness Plan.

Annex I: Presenting the Results of the Industry Consultation

On 26 July 2021, the HEA put forward the draft of the Hungarian Electricity Supply Risk Preparedness Plan for industry consultation. The Authority accepted comments and suggestions from industry players and sectoral organisations electronically until 26 August 2021. On the HEA's website, a permanent notice box called the attention of the industry players to the consultation during the reference period.

The link announcing the public consultation:

http://www.mekh.hu/iparagi-konzultacio-a-magyar-villamosenergia-ellatasi-kockazati-keszultsegi-tervrol

Answering the call of the Hungarian Energy and Public Utility Regulatory Authority, four industry players and organisations submitted comments during the reference period.

Therefore, the Risk Preparedness Plan is hereby appended with a description of the industry consultation process, the opinions received, and the manner in which they were taken into account.

The purpose of this Annex is to describe the opinions received during the consultation and the results of these opinions being taken into consideration by the Authority in detail.

The comments received from one of the participants were considered by the Authority but were found to be unsuitable to be taken into account during the process of updating the plan due to a lack of relevance; therefore, the HEA will forego presenting them in this Annex.

The Authority hereby provides the following information regarding the industry proposals received and their evaluation by the HEA:

Industry Opinion Received	Feedback of the Authority
One of the participants requested that in the chapter discussing the Member States located in the region (1.2), Hungary was also included.	The Authority accepts the proposal and amends the relevant chapter of the Plan accordingly.
One of the participants requested that pursuant to the paragraph of Chapter 4.1 on the flow of information, it was not the licence holder that was required to contact the County Disaster Control Directorates in the event of a crisis but the other way around, the County Disaster Control Directorates contacted the licence holders.	The Authority states that it is not authorised to deviate from the effective provisions of the applicable industry legislation and regulations when preparing the Plan and recommends the submission of this comment to the competent organisation (Crisis Working Committee).
One of the participants requested that in the case of the applicability of Section h) of Chapter 4.2 Tasks of the transmission system operator related to preparing for a crisis and during a crisis, in addition to the electricity settlement, the system-level services utilised during a crisis were also mentioned among the settlement obligations. Furthermore, the participant asked which principles should be	The Authority would like to highlight that it is not practical to break down further the settlement of the electricity supplied to and consumed through the grid based on additional market segments during a period of significant disruption and would like to add that this applies to the settlement of system-level services as well.

taken into account in cases where the transmission system operator uses units that were not subject to a valid contract (no commercial option has been assigned thereto).	To the best of the Authority's knowledge, the TSO enters into at least an optional contract with the operators of all units that are accredited to be used for the provision of system-level services.
One of the participants expressed that in its opinion, the preventative and crisis management measures listed in the table included in Chapter 4.5.3 were incomplete, vague, or impractical (unfeasible) in several places. A non-exhaustive list of these measures: - Establishment and maintenance of an alternative (backup) control centre - Preparing equipment for operation in expected extreme winter weather conditions - Preparing equipment for operation in expected heatwave and extreme hot weather conditions - Preparing for water extraction with adequate safety during low water periods by installing flexible water abstraction structures and devices.	The Authority states that the implementation of the provisions of Chapter 4.5.3 is a forward-looking expectation towards the goal of reinforcing risk preparedness; it is to be achieved and tracked gradually. In particular, the preparation of equipment for the extreme winter weather or hot weather conditions is an already existing requirement; therefore, the Authority does not consider it justified to deviate therefrom. However, the Authority does agree with the participant in that the establishment and maintenance of an alternative (backup) control centre would result in disproportionate costs and provide only moderate benefits in terms of actual security risk reduction; therefore, the Authority hereby authorises the removal of the provision from the Plan.
One of the participants expressed that the study presented the key risk factors in detail and focuses on system operation and key power plants. The comment of the participant was that with the spread of the already widely-used decentralised household and small power plant (solar panel) systems, the built-in units might carry risk factors that the study did not deal with. There are currently several tens of thousands of inverters already in operation in Hungary, the vast majority of which is online. In the online space, the maintenance and monitoring of these systems become easier for manufacturers and customers. There have been examples of certain manufacturers accessing the inverter remotely and without the	In its response, the Authority states that the introduction of additional requirements in excess of the existing legislation applicable to the widespread decentralised household and small power plant (solar panel) systems in the Risk Preparedness Plan would create excessive administrative and other burdens for the parties operating such units; however, the HEA acknowledges that the aggregated ratio of these power plants already has an important effect on the operation of the power grid. In this regard, the Authority foresees the expected expansion of the operating and commercial regulations of the European Union, where an operating and commercial regulation on cyber security rules for the cross-border electricity networks is already under development. The regulation will

knowledge of the customer and implementing modifications therein. This advantage can clearly carry vulnerabilities as well if it falls into unauthorised hands. In just a few seconds, Hungary could be disconnected from the EU network or shut down the entire grid through a sudden frequency increase or reduction. In extreme cases, this could even have effects on the European network. The participant proposed the inclusion of the product and cyber security risks of built-in devices in the study, thus drawing attention to minimising this vulnerability.	include the **assessment of the cyber security risks (risk index) of electricity industry undertakings** based on a unified methodology, the investigation of the security of the cross-border capacity flows using a unified cyber risk methodology, and **the introduction of a common cyber security framework for ensuring a minimally required cyber security protection level.** After this regulation has entered into force, the Authority is going to revise its Risk Preparedness Plan if necessary in order to ensure that the new cyber security provisions are transposed into the Plan as well.
One of the participants expressed that it had reviewed the draft and it did not have any conceptional remark in regard thereto. However, it wished to draw the attention of the Authority to an anomaly already known to the HEA, which exists as a contradiction between the provisions of Section 13 (2) and 14 (3) of Government Decree 280/2016. (IX.21.). In light of the industry consultations already underway with respect to this issue, the participant recommended that the stipulation pertaining to the restriction of essential users was only included in the draft after this issue has been appropriately reconciled and the stipulation should reflect the results of the reconciliation.	The Authority states that it has submitted an amendment proposal concerning the relevant provisions of Government Decree 280/2016. (IX.21.) in connection with the restriction of essential users, which would address the questions raised by the network licence holders. As soon as the Authority obtains definitive information on the amendment of the Government Decree, it is going to contact the affected network licence holders and amend the Plan accordingly.
One of the participants requested that the extraordinary events specified in Government Decree 374/2020. (VII. 30.) on the identification, appointment, and protection of essential energy systems and facilities were also included in the introductory section of the Plan. With respect to the same section, the participant proposed that the fulfilment of the provision included in Section 6 (17) of Government Decree 374/2020. (VII. 30.) on the identification, appointment, and protection of essential energy systems and facilities was also listed, according to which "with the exception of essential national defence system components within the industry, the operators	The Authority states that the sectoral scope of this Risk Preparedness Plan, as well as the measures and crisis scenarios included therein, is not identical to the scope of industry licence holders appointed pursuant to Government Decree 374/2020. (VII. 30.) on the identification, appointment, and protection of essential energy systems and facilities; therefore, such unification of the crisis scenarios is not justified.

of essential European system components and essential European system components and the sectoral appointing authority shall submit the electronic data of their registration and supervisory systems to the competent disaster management body within 60 days of the appointing resolution becoming final and enforceable, which serve as evidence of the capacity of the competent disaster management bodies cooperating on the performance of the damage mitigation activity to respond immediately, as well as facilitate successful intervention and recovery."	
One of the participants noted that the definition of relevance applicable to scenarios (Chapter 2) could be interesting in the case of certain scenarios. This is due to the fact that both potential severity and the likelihood of occurrence could change rapidly, which could be easier to track this way. Furthermore, in regard to the sub-indicators used for the measurement of relevance, the definitions determining which category each of them falls into would be useful in the form of a Glossary.	The Authority states it does not consider it justified to further break down the definition levels of relevance, which is consistent with the methodology of the ENTSO-E in its current form; however, it would like to add that there are going to be opportunities for amending the relevance of the future scenarios referred to by the participant, which are also going to be obligatory in accordance with the provisions of the Risk Preparedness Regulation as Plans are required to be updated every four years.
One of the participants proposed (in a comment made with respect to Chapter 2) that in order to ensure clarity, this definition and all other definitions used in the Plan should be compiled into and defined in a Glossary, which would constitute a part of the Plan. Furthermore, as a part of such a Glossary, the participant proposed that the ICS covered by this definition were also specified (including the base, emergency operation, and uninterrupted power supply thereof). In general, the participant proposed the increased protection of the power supplies since a successful attack against these would result in all other ICS also becoming inoperable, as opposed to an attack against other ICS.	The Authority states that the use and meaning of the terms and definitions in the Plan can be clearly identified on a systemic level; therefore, it does not consider it justified to introduce a glossary. No similar comment was received by the Authority from any other industry licence holder or system user either.
With respect to the scenario concerning cyber security, one of the participants put forward that it was necessary to clarify the term as not all incidents are cyber-attacks but all cyber-attacks are incidents. Furthermore, the participant recommended that the scope of the Plan was extended to apply to incidents as well.	The Authority states that in the scenario, the term "cyber-attack" is clearly defined as an intentional and deliberate act aimed at causing damage, while in the case of incidents, the aim of deliberately causing damage is not clear; therefore, the HEA does not plan to amend the title of the crisis scenario.

With respect to the scenario concerning cyber-attacks, one of the participants proposed that it would be worth preparing for the future expansion of the list of players (e.g. aggregator) named in the scenario, which could naturally apply to the other scenarios as well.	The Authority states that it agrees with the opinion on the necessary expansion of the list of affected players (e.g. aggregators) in time in the case of all relevant scenarios. Taking into account the fact that the detailed rules applicable to aggregators and other new players are currently under development on the regulatory level and in order to eliminate the obstacles for market entry of new players, this will be necessary to be investigated during the review of the Plan, which is required to be performed at least every four years.
One of the participants proposed with respect to the title of Chapter 2.1 that the term "business" might be redundant and could have been the basis for misunderstandings as the Chapter does not deal with electricity trade or other business processes (simple data reporting) but all critical ICT systems (including the central SCADA system).	The Authority agrees with the opinion of the participant and amends the title of the Chapter in the Plan accordingly.
One of the participants proposed with respect to the description of Chapter 2.1 that in order to ensure clarity, an itemised list of the affected systems should be included here and/or in the Glossary proposed earlier instead of mentioning only a number of examples. Furthermore, the participant stated that in accordance with the lower levels of the Purdue model*, the scope of the Plan should include devices (e.g. protective equipment, automated systems), which were no less important from the point of view of security of supply. The inclusion of system-level automated systems was also recommended. Furthermore, the participant proposed the clarification and narrowing down of the vague term of "office IT devices". *Purdue model: see Chapter 7.1 of the Cyber Security Handbook of Supervisory Systems in the Electricity Industry. The list is not "homogenous"; attacks against practically any device could be included here based on it. This is not necessarily an issue but the intention is not clear from the text.	The Authority states that an itemised list of the affected systems is not justified due to the fact that it might lead to a limited interpretation of the scenario, and it would make it more difficult to consider the new system components that may emerge between the four-year review periods as well.
With respect to the description of Chapter 2.1,	The Authority agrees with the proposal;

one of the participants proposed that the role of country borders (or more accurately, TSO borders) was essential in the EU-level regulations. Furthermore, in the Preparedness Plan, we could prepare for inter-organisation effects as well (meaning that an attack on a DSO could have a significant effect on the TSO for example, or vice versa, not only from a business operational point of view but from the viewpoint of cyber-attacks as well).	therefore, the Risk Preparedness Plan includes the management of the cooperation and interactions between individual players as well.
With respect to the description of Chapter 2.2, one of the participants suggested that physical attacks against the information communication infrastructure were left out from the list. The results may be similar to that of a loss of load (see Chapter 2.10) but the likelihood of occurrence may be different.	The Authority states that Chapter 2.10 "Loss of critical information and communication technology infrastructure" addresses the question raised to a sufficient extent; therefore, amending the title of Chapter 2.2 is not justified.
With respect to scenario 2.3, one of the participants proposed that the list should include the role of aggregators as well, which would become ever more important in the near future (as well as virtual power plants and control centres).	The Authority states that it agrees with the opinion on the necessary expansion of the list of affected players (e.g. aggregators) in time in the case of all relevant scenarios. Taking into account the fact that the detailed rules applicable to aggregators and other new players are currently under development on the regulatory level and in order to eliminate the obstacles for market entry of new players, this will be necessary to be investigated during the review of the Plan, which is required to be performed at least every four years.
With respect to scenario 2.7, one of the participants raised the issue that no specified "recovery time" was provided in the case of other scenarios, thus it appeared overly specific in this case: in a situation exasperated by nationwide flooding and landslides, the rebuilding of the physical infrastructure might take longer than this.	The Authority agrees with the opinion and amends the period (one month) specified for scenario 2.7 to allow for a more generalised interval.
With respect to scenario 2.7, one of the participants proposed that this (note: the business continuity of fossil-fuel mining) was uncommon in Hungary; therefore, it would be possible to list specifically which power plants the Plan applies to.	The Authority states the provisions of the Risk Preparedness Plan apply to the industry licence holders specified in the applicable legislation; therefore, it is not justified to include or name specific undertakings in the Plan.
With respect to scenario 2.10, one of the participants noted that this scenario discusses "information communication device", while Section 2.1 of the Plan includes the term "information communication systems". The participant proposed the use of uniform terms.	The Authority approves the proposal and amends the Plan accordingly (to uniformly include the term "information communication systems").

With respect to scenario 2.10, one of the participants put forward that in extreme cases (such as the attacks in Ukraine in '15 and '16), system recovery was performed using on-site coordination, that is remote verbal instructions given to operating personnel at the substation. "Controlled" switching would imply switching by dispatchers in the case of operational ICS instead.	The Authority acknowledges the opinion but does not consider it justified to amend the Plan.
With respect to scenario 2.10, one of the participants suggests that this (note financial losses sustained by market players) could happen in the case of any scenario event. It is recommended to standardise the effects and evaluate the scenarios based on identical criteria. E.g. if a recovery time is specified for one, it should be specified for all of them.	The Authority states that it is unfeasible for the description of and information provided with respect to the scenarios to include all effects that may arise when the scenario occurs; therefore, the HEA attempted to include the criteria during the description of the scenarios that are directly related to the specific scenarios in question.
With respect to scenario 2.11, one of the participants suggested that this situation may occur for reasons other than those listed as well: e.g. a coordinated attack against smart home controllers or a sudden power spike caused by vehicle chargers.	The Authority acknowledges the opinion but does not consider it justified to amend the Plan.
With respect to scenario 2.13, one of the participants put forward that the effects of the scenario may include not only excess capacities but shortages as well, and a need for load increases, not only load reductions.	The Authority approves the proposal and amends the description of the scenario accordingly.
With respect to scenario 2.15, one of the participants put forward that the effects listed primarily occur on the European level; therefore, it would be helpful to provide more details in regard to the Hungarian circumstances.	The Authority states that the national scenario is in line with the regional scenarios; therefore, it is more practical to provide the effects and the description of the scenario using the same approach. Therefore, the HEA does not consider the amendment of the Plan to be justified.
With respect to scenario 2.16, one of the participants put forward that the effects listed primarily occur on the European level; therefore, it would be helpful to provide more details in regard to the Hungarian circumstances.	The Authority states that the national scenario is in line with the regional scenarios; therefore, it is more practical to provide the effects and the description of the scenario using the same approach. Therefore, the HEA does not consider the amendment of the Plan to be justified.
With respect to scenario 2.18, one of the participants stated that it does not understand the relevance of this sentence (note: the occurrence of the scenario is more likely in Southern Europe) to the Hungarian scenario; the likelihood of occurrence in Hungary should be assessed here.	The Authority agrees with the opinion and removes the sentence concerned from the Plan.
With respect to Chapter 3.1, one of the	The Authority states that it is not authorised

participants enquired whether the role of aggregators is included with that of electricity traders here, taking the composition of the Crisis Working Committee into account.	to deviate from the provisions of the effective legislation. Furthermore, the appearance of new players is required to be investigated continuously in the course of the review process of the effective legislation and in the event of an amendment, the Plan may be required to be updated at least every four years; therefore, during the updating procedure, the investigation is required to include the industry players newly included in the scope of the legislation.
With respect to Chapter 3.1, one of the participants suggested that there were not enough details included in regard to the crisis simulation practices and thus the contents of the scenario should be expanded.	The Authority states that the schedule of the biannual regional (and if applicable, national) real-time simulations of the responses to electricity supply crises is currently under development (in accordance with Chapter 7).
With respect to Chapter 3.1, one of the participants noted that the performance of crisis (simulation or other) practices was not included here (note: the tasks of the DSO).	The Authority states that the schedule of the biannual regional (and if applicable, national) real-time simulations of the responses to electricity supply crises is currently under development; however, these concern the coordination of the cooperation between TSOs in particular (in accordance with Chapter 7).
One of the participants proposed the supplementation of Chapter 4.1 (note: System protection plan) as follows: "The aim of the plan is to prepare for and prevent the occurrence of possible major – even continent wide – system failures..."	The Authority states that the basic geographical scope of the system protection plan is Hungary and the Hungarian power grid; however, taking the international connections of the power grid and the interoperable European electricity system into account, the HEA approves this proposal and amends the Plan accordingly.
With respect to Chapter 4.2, one of the participants proposed that it would be necessary to consult with the stakeholders of other regulations and plans in regard to the list of parties to be notified in this case (note: "(a) shall report to the Minister for Innovation and Technology and the President of the Authority and inform the members of the CC of the occurrence, cause and expected duration of the significant disturbance"). For example, the Minister for Innovation and Technology is not included in the crisis plan of MAVIR. This could remain "the minister responsible for energy policy" just like in the crisis plan.	The Authority states that the name of the Ministry is consistent with the list of state organisations (under Chapter 4.6); therefore, it does not consider the adoption of this proposal to be necessary.
With respect to Chapter 4.5.1.1, one of the participants proposed that the activity (note:	The Authority agrees with the proposal and amends the Plan accordingly.

crisis management regulation) should be moved over to the "Preventative measures" column.	
With respect to Chapter 4.5.1.5, the opinion of one of the participants was that the logical relation of "or" should be reviewed. The OSP and ISP already include the regulation of permissions, as well as other issues listed before the word "or".	The Authority agrees with the proposal and amends the Plan accordingly.
With respect to Chapter 4.5.2.1, one of the participants proposed an addendum to the wording provided therein: "In the first part of the scenario, the attack possibilities against the systems specified therein are to be considered..." Furthermore, the participant proposed the inclusion of an itemised list of the affected systems and their identification based on their level in the Purdue model. This would allow for the identification of the IT and OT systems and their affected components.	The Authority states that an itemised list of the affected systems is not justified due to the fact that it might lead to a limited interpretation of the scenario, and it would make it more difficult to consider the new system components that may emerge between the four-year review periods as well.
With respect to Chapter 4.5.2.1, the opinion of one of the participants was that here (note: Crisis management measures), the scenario and the previous column clearly included the SCADA system; therefore, this sentence contradicted the previous provisions (the SCADA system and the information communication infrastructure, in general, serve not only market activities).	The Authority states that the sentence does not contradict the previous column; it is consistent with the first part of the scenario included in the previous column. The Authority supplements the list of crisis management measures with respect to the second part of the scenario as well.
The opinion of a participant concerning Chapter 4.5.2.1 was that it would be beneficial to include a detailed evaluation of the attacks relevant from time to time (e.g. Ukrainian or Saudi Arabian attacks), together with what can be learned from them and what necessary measures might have to be taken as a preventative measure.	The Authority states that Paragraph 4.5.2.1 "Preventative measures" suitably addresses the concerns of the participant as the Subchapter includes the following: The mutual sharing of relevant information (on threats and security events and incidents) among the TSO's cybersecurity protection activities in a closed circle, in particular with cyber security experts from European system operators, is of particular importance, as these resources can provide a wealth of information that will allow for faster and more effective action in the event of a wider cyber-attack (against all or part of the European electricity system).
The opinion of a participant concerning Chapter 4.5.2.1 was that the note included in parentheses should be reconsidered as this does not necessarily apply to the devices and systems belonging to the lower levels of the	The Authority approves the proposal and amends the Plan accordingly.

Purdue model.	
The opinion of a participant concerning Chapter 4.5.2.1 was that this (note: only users with appropriate authorisation can access it) cannot be guaranteed, only steps taken to ensure it, this is exactly why the case discussed in the scenario is important.	The Authority acknowledges the opinion but does not consider it justified to amend the Plan.
The opinion of a participant concerning Chapter 4.5.2.3 was that the contents of "internal procedures" or "internal regulations" were not clear from the point of view of an external reader; therefore, making it difficult to evaluate whether the preparedness is sufficient.	The Authority acknowledges the opinion but does not consider it justified to amend the Plan due to the protection of the sensitive information included in internal procedures.
With respect to Chapter 4.6, one of the participants expressed the opinion that in this case (note: state organisations), it would once again be beneficial to standardise the list of players included in the various materials; the crisis plan of MAVIR still includes the Ministry of National Development not the Ministry of Innovation and Technology.	The Authority states that the name of the Ministry is consistent with the list of state organisations (under Chapter 4.6); therefore, it does not consider the adoption of this proposal to be necessary.
A question of a participant concerning Chapter 4.6 was whether "traders with a ratio of turnover from the electricity sector of more than 5%" were left out of this paragraph (note: system users).	The Authority agrees with the proposal and amends the Plan accordingly.


MEKH
Hungarian Energy and Public
Utility Regulatory Authority

2022