MINISTRY
OF ECONOMY
OF THE SLOVAK REPUBLIC

Risk-preparedness plan of the Slovak Republic for the electricity sector

(pursuant to Regulation (EU) 2019/941 of the European Parliament and of the Council on risk-preparedness in the electricity sector)

December 2021

Table of contents

List of abbreviations

TSO	transmission system operator
DSO	distribution system operator
AnS	ancillary service
ES	electricity system
TS	transmission system
DS	distribution system
RONI	Regulatory Office for Network Industries
SEPS	Slovenská elektrizačná prenosová sústava, a.s. - transmission system operator
OKTE	Organizátor krátkodobého trhu s elektrinou, a.s. - short-term electricity market operator
MoE	Ministry of Economy of the Slovak Republic
ICT	information and communication technologies
RES	renewable energy sources
ENTSO-E	European Network of Transmission System Operators for Electricity
NSA	National Security Authority

List of national legislation

Act No. 251/2012 Coll. on the energy sector and on amendments to certain acts

Ministry of Economy Decree No. 416/2012 Coll. laying down the details on the procedure for the application of restrictive measures in emergency and on measures designed to eliminate emergency in the electricity sector and the details on the procedure regarding the declaration of emergency and its level, the deceleration of restrictive gas sector measures for individual categories of gas customers, on measures designed to eliminate the crisis situation and on the manner of speciation of restrictive measures in the gas sector and measures designed to eliminate the crisis situation

Act No. 69/2018 Coll. on cybersecurity and on amendments to certain acts

Act No. 45/2011 Coll. on critical infrastructure

Act No. 128/2015 Coll. on prevention of serious industrial accidents and on amendments to certain acts

Act No. 110/2004 Coll. on the functioning of the Security Council of the Slovak Republic at the time of peace

1. GENERAL INFORMATION

1.1 Competent authority

In line with the requirement under Regulation (EU) 2019/941 of the European Parliament and of the Council on risk-preparedness in the electricity sector (hereinafter only referred to as the "Risk-preparedness Regulation"), the competent authority of a Member State has an obligation to draw up a risk-preparedness plan on the basis of the regional and national electricity crisis scenarios.

The competent authority in Slovakia is the Ministry of Economy of the Slovak Republic (hereinafter only referred to as the "MoE").

The risk-preparedness plan should be developed in accordance with Articles 11 and 12 of the Risk-preparedness Regulation and with the template set out in its Annex. The aim is to identify national electricity crisis scenarios, examine their possible impact on the operation of the electricity system, and set out measures to resolve or prevent electricity crisis.

1.2 Member States in the region and international cooperation

The Slovak Republic has direct cross-border connections with the electricity systems in the Czech Republic (3 x 400kV and 2 x 220kV), Hungary (5 x 400kV), Poland (2 x 400kV), and Ukraine (1 x 400kV). Agreement on Grid and System Operation Management and General contract for emergency deliveries have been signed with these countries at the level of transmission system operators (hereinafter only referred to as "TSOs"). The competent authority shall also inform other Member States in the framework of cross-border conventions of the causes of a possible electricity supply crisis, measures planned or taken to prevent an electricity supply crisis and the possible need for emergency assistance.

As part of the so-called Core region (TSOs from Germany, France, Belgium, the Netherlands, Luxembourg, Poland, Austria, Hungary, the Czech Republic, Portugal, Spain, Italy, Romania, Slovenia, and Croatia), the Slovak TSO is engaged in cooperation in security analyses, coordination plans of the outages, remedial actions, or joint regional methodologies. Certain measures under defence plans or restoration procedures after a system breakdown or blackout (top-down restoration procedure) are also defined in the Continental Europe Synchronous Area Framework Agreement (hereinafter only referred to as "SAFA").

2. SUMMARY OF THE ELECTRICITY CRISIS SCENARIOS

2.1 Consultations and selection of national crisis scenarios

Under Article 7(1) of the Risk-preparedness Regulation, the competent authority shall identify the most relevant national electricity crisis scenarios by 7 January 2021. The scenarios must be based on the regional crisis scenarios published by the European Network of Transmission System Operators (ENTSO-E) on 7 September 2020. The national electricity crisis scenarios should be selected in cooperation with the transmission system operator and in consultations with distribution system operators (hereinafter only referred to as the "DSOs"), relevant producers or their trade bodies, and the regulatory authority (Article 7(2)).

The MoE in cooperation with the TSO, Slovenská elektrizačná prenosová sústava, a.s. (hereinafter only referred to as "SEPS"), had identified the highest-risk crisis scenarios that were submitted to Regulatory Office for Network Industries (hereinafter only referred to as the "RONI") and to the relevant market participants for consultations. The regional and national crisis scenarios were identified in compliance with the "Methodology to Identify Regional Electricity Crisis Scenarios in accordance with Article 5[1]" prepared by the ENTSO-E.

Of the total of 31 regional scenarios identified in a non-public ENSTO-E document ("Identification of Regional Electricity Crisis Scenarios"), twelve scenarios posing the highest risk to the operation of the Slovak electricity system were chosen as national crisis scenarios.

National scenarios have been divided into five groups according to their characteristics. A common denominator are similar procedures employed to remove the impacts of these scenarios, or to prevent and avoid formation and escalation of the crisis situation.

Tab. 1 List of national crisis scenarios for Slovakia

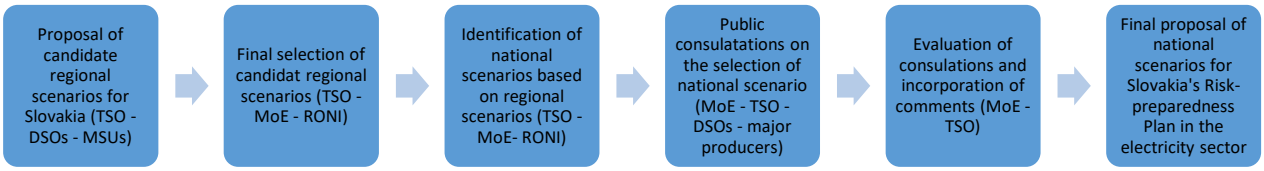
	National scenario name
Group 1	(1) A cyberattack against the critical business ICT infrastructure of the entities connected to the electricity system, such TSOs, DSOs, power plants, and large (industrial) customers
	(2) A cyberattack against the important business ICT infrastructure in market participants (not physically connected to the electricity system)
	(6) Insider attack
	(17) The loss of ICT systems for real-time operation
Group 2	(5) Threat to key employees
	(23) Strike, riots, industrial action
Group 3	(10) Cold spell
	(16) Multiple failures caused by extreme weather
	(28) Heatwave
	(29) Dry period
Group 4	(27) Pandemic
Group 5	(24) Industrial/nuclear accident

[1] https://consultations.entsoe.eu/system-operations/risk-preparedness-regulation-methodology-for-ident/

The proposal for national crisis scenarios was consulted with the relevant market participants pursuant to Article 7(2) of the Risk-preparedness Regulation at a meeting held on 16 December 2020. The following market participants and institutions were represented at the consultation meeting:

- National regulatory authority
  - Regulatory Office for Network Industries
- Transmission system operator
  - Slovenská elektrizačná prenosová sústava, a.s.
- Regional distribution system operators
  - Východoslovenská distribučná, a.s.
  - Stredoslovenská distribučná, a.s.
  - Západoslovenská distribučná, a.s.
- Major operators of electricity generation facilities
  - Slovenské elektrárne, a.s.
  - ZSE Elektrárne, s.r.o.
  - Vodohospodárska výstavba, š.p.

Step-by-step identification and selection of national crisis scenarios under the Risk-preparedness Plan:



2.2 Description of national crisis scenarios

2.2.1 Rating method for the severity of crisis scenarios

The evaluation of the crisis scenario, its cross-border dependencies and resulting severity in terms of risk to the supply of electricity has been conducted using the procedure specified the ENTSO-E methodology[2]. The rating of the impact of the crisis scenario consists of likelihood of occurrence, loss of load expectation (LOLE) per year, and expected energy not supplied (EENS) in GWh per year. The cross-border dependency assesses the ability of an incident to spread across the borders of the territory of the Slovak Republic and have impacts on neighbouring interconnected power systems. The overall rating of the severity of the scenario is calculated as follows:

$$Overall\ rating = Crisis\ scenario\ rating * Crossborder\ dependency\ rating$$

Crisis scenario rating	Value
Disastrous	10
Critical	5
Major	2
Minor	1
Insignificant	0

[2] https://consultations.entsoe.eu/system-operations/risk-preparedness-regulation-methodology-for-ident/

Cross-border dependency rating	Value	Description
None	1	The crisis has no impact on neighbouring countries, even if they are facing simultaneous or coincident crisis.
Minor	1,2	The crisis is susceptible to aggravate a simultaneous or coincident crisis in at least one of the neighbouring countries, either through direct or indirect causes.
Major	2	The crisis is susceptible to generate a cross-border crisis in at least one of the neighbouring countries, either through direct or indirect causes.

2.2.2 Description of national crisis scenarios

(1) A cyberattack against the critical business ICT infrastructure of the entities connected to the electricity system, such TSOs, DSOs, power plants, and large (industrial) customers

Scenario:

A cyberattack against the SCADA system and control systems with their subsequent disruption. Control rooms do not receive real-time data, and/or the validity of the data on the ES status cannot be guaranteed in the real time, and the system management is considerably restricted. Such disruptions make the system management dysfunctional and the system is running without the possibility of intervention, and/or without correct decisions from control rooms. If an unexpected situation occurs, there is a risk that the problem will be incorrectly identified, followed by a failure/outage of an element of the system, which may lead to a cascading outage of installations and subsequently cause a blackout.

Scenario evaluation:

Crisis scenario rating	Cross-border dependency rating	Overall rating
Minor	Major	2

Scenario evaluation in words:

The cross-border energy exchange and reserve sharing may be at serious risk if the attack focuses on cross-border infrastructure facilities and installations. Combined with adverse circumstances, such as adequacy problems, this could result in triggering an automatic demand disconnection and interruption of cross-border electricity exchanges. The impact depends on the size and severity of the attack and on whether it will be carried out gradually, or with a strong force and extent over a short time. It is highly probable that the attacker intends to make the largest possible impact and restrict the users' consumption as much as possible.

(2) A cyberattack against the important business ICT infrastructure in market participants (not physically connected to the electricity system)

Scenario:

A cyberattack against market participants, e.g., an electricity exchange market. The volume of electricity traded does not match the real values. The electricity not delivered or not taken must be substituted through ancillary services. If the available ancillary and emergency assistance services are exhausted and the situation further deteriorates, electricity emergency must be declared and all available options used in order to preserve the system's synchronous operation. The cyberattack against the electricity exchange market may also cause unexpected transit flows between the transmission systems that will overload interconnectors, and subsequent problems with complying with the N-1 security criterion.

Scenario evaluation:

Crisis scenario rating	Cross-border dependency rating	Overall rating
Minor	Major	2

Scenario evaluation in words:

The cross-border energy exchange and reserve sharing may be at serious risk because the attack is very likely to be directed against a market participant with a strong market influence. Combined with adverse circumstances, such as adequacy problems, this could result in triggering an automatic demand disconnection and interruption of cross-border electricity exchanges. The impact depends on the size and severity of the attack, and on whether it will be carried out on an entity with a low or high impact on balancing in Slovakia's electricity system. It is highly probable, however, that the attacker intends to make the largest possible impact and restrict the users' consumption as much as possible.

(5) Threat to key employees

Scenario:

A critical infrastructure employee finds himself/herself in a tense situation where he/she is forced by a third person to take, out of the fear for his/her health and life and for the life of his/her close persons, such system management actions that will result in the outage of multiple elements of the electricity system. The system becomes unstable and the supply of electricity is interrupted. The situation may have a negative impact on the neighbouring power systems, as well.

Scenario evaluation:

Crisis scenario rating	Cross-border dependency rating	Overall rating
Major	Major	4

Scenario evaluation in words:

The cross-border energy exchange and reserve sharing may be at serious risk if the attack targets an employee authorised to access systems ensuring stable operation in the extent that affect cross-border cooperation. Combined with adverse circumstances, such as adequacy problems, this could result in triggering an automatic demand disconnection and interruption of cross-border electricity exchanges. The impact depends on the size and severity of the attack and on whether it will be carried out gradually, or with a strong force and extent over a short time. It is highly probable that the attacker will force the hostage to make an intervention with the largest possible impact and restricting the users' consumption as much as possible.

(6) Insider attack

Scenario:

The management information system or management support systems are deliberately damaged at a physical or logical level through a professional intervention performed by a person with access rights. The intervention disables the management of system elements, shuts them down, makes data invalid with the aim of disrupting the generation and/or supply of electricity.

Scenario evaluation:

Crisis scenario rating	Cross-border dependency rating	Overall rating
Critical	Major	10

Scenario evaluation in words:

The cross-border energy exchange and reserve sharing may be at serious risk if the attack is undertaken by an employee authorised to access systems ensuring stable operation in the extent that affect cross-border cooperation. Combined with adverse circumstances, such as adequacy problems, this could result in triggering an automatic demand disconnection and interruption of cross-border electricity exchanges. The impact depends on the size and severity of the attack and on whether it will be carried out gradually, or with a strong force and extent over a short time. It is highly probable that the attacker will make an intervention with the largest possible impact and restricting the users' consumption as much as possible.

(10) Cold spells

Scenario:

Low water levels and freezing shut down hydropower plants. Nuclear and thermal power plants must operate in a restricted regime due to the lack of water in cooling tanks. The increased demand for electricity puts the system into deficit. Transmission lines are covered by ice due to low temperatures. Cross-border interconnectors are at a risk of outage which may lead to the loss of the possibility to import electricity from abroad.

Scenario evaluation:

Crisis scenario rating	Cross-border dependency rating	Overall rating
Major	Minor	2,4

Scenario evaluation in words:

The scenario has an overall significant risk profile with a lesser risk of cross-border impact. Experts have assessed the incident as likely, mainly having impact on the restriction of consumption, as well as with effect on cross-border transfers, therefore it is evaluated as major. Combined with adverse circumstances, such as planned shutdowns and unscheduled emergency shutdowns, manual or automatic demand disconnection is likely to be triggered. The impact on the restriction of consumers depends on the possibility of importing electricity from foreign power systems.

(16) Multiple failures caused by extreme weather

Scenario:

An extreme heat wave results in the overheating and subsequent outage of several transmission transformer substations simultaneously and disrupts the supply of electricity to nodal areas. The lack of water results in the outage of major electricity sources. Strong winds damage major interconnectors over a short time interval. The system lacks electricity and its import from abroad is limited.

Scenario evaluation:

Crisis scenario rating	Cross-border dependency rating	Overall rating
Major	Minor	2,4

Scenario evaluation in words:

The scenario may have an impact on consumption restriction, as well as on cross-border transfers, and is evaluated as major. Combined with adverse circumstances, such as planned shutdowns and unscheduled emergency shutdowns, a manual or automatic demand disconnection is likely to be triggered. The impact on the restriction of consumers depends on the possibility of importing electricity from foreign power systems.

(17) The loss of ICT systems for real-time operation

Scenario:

The loss of ICT systems causes that employees in the operative management cannot verify information. They cannot communicate with electricity producers, large industrial customers, and providers of ancillary services.

Scenario evaluation:

Crisis scenario rating	Cross-border dependency rating	Overall rating
Minor	Minor	1,2

Scenario evaluation in words:
Power system management is largely restricted. If an operative intervention in the system's operation is needed and that intervention cannot be carried out, the cross-border exchange and reserve sharing may be limited which, combined with adverse circumstances, such as adequacy problems, could result in triggering an automatic demand disconnection and interruption of cross-border electricity exchanges. The impact depends on how long the system management has been limited in real time.

(23) Strike, riots, industrial action
Scenario:
A strike of energy sector workers results in the outage of several major sources, refusal to manage the system, or trade in electricity.

Scenario evaluation:

Crisis scenario rating	Cross-border dependency rating	Overall rating
Major	Major	4

Scenario evaluation in words:
With an incident under this scenario, there is a chance that the possibility to maintain the system's stability will be limited, be it in terms of transmission and distribution, or in terms for sources or unstable supply for large customers. These events may have an impact on the cross-border energy exchange, reserve sharing, as well as on restrictions on electricity supply to system users. The size of the impact will depend on the size of the personnel on strike and on the area of the company's operation.

(24) Industrial/nuclear accident
Scenario:
A nuclear plant accident with radiation leak. A major source outage. The accident contaminates a wide area around the power plant, affecting another power plant in the system to which employees are denied access – power plant is put out of operation. Access to the control centre from a distribution system is also impossible.

Scenario evaluation:

Crisis scenario rating	Cross-border dependency rating	Overall rating
Major	Major	4

Scenario evaluation in words:
With an incident under this scenario, there is a chance that the possibility to maintain the system's stability will be limited, be it in terms of transmission and distribution, or in terms for sources or unstable supply for large customers. These events may have an impact on the cross-border energy exchange, reserve sharing, as well as on restrictions on electricity supply to system users. The size of the impact will depend on the size of the contaminated area and the number of entities affected. If this event occurs, one must expect that the operation of affected entities will be limited for a long time.

(27) Pandemic
Scenario:
A critical infrastructure employee (e.g., a control room operator) contracts the infection. The disease prevents him/her from performing his/her official duties. Employees who have been in contact with an infected individual must be quarantined. The spreading of the disease was not prevented in time and workers on other shifts have been infected. Back-up shifts cannot make up for the lost personnel. The exhaustion of the remaining personal causes an increase in erroneous decisions.

Scenario evaluation:

Crisis scenario rating	Cross-border dependency rating	Overall rating
Major	Major	4

Scenario evaluation in words:

With an incident under this scenario, there is a chance that the possibility to maintain the system's stability will be limited, be it in terms of transmission and distribution, or in terms for sources or unstable supply for large customers. These events may have an impact on the cross-border energy exchange, reserve sharing, as well as on restrictions on electricity supply to system users. The size of the impact will depend on the number of employees incapable to perform their duties and the number of affected entities. If this event occurs, one must expect that the operation of affected entities will be limited for a long time.

(28) Heatwave

Scenario:

Low water levels cause a reduction/outage of hydropower plants' generation capacities. Pumped-storage hydropower plants cannot operate, either. Thermal and nuclear power plants operate under a restricted regime due to the low volumes of cooling water in the tanks. Transmission system elements, such as transformers and power lines, are overheating. Cross-border interconnectors are at a risk of outage which may lead to the loss of the possibility to import electricity from abroad. The increased demand for electricity, driven by cooling installations and domestic air-conditioning systems, puts the system into a considerable deficit.

Scenario evaluation:

Crisis scenario rating	Cross-border dependency rating	Overall rating
Critical	Major	10

Scenario evaluation in words:

The incident would mainly have an impact on the restriction of production and on cross-border transfers; the impact is evaluated as critical. Combined with adverse circumstances, such as planned shutdowns and unscheduled emergency shutdowns, a manual or automatic demand disconnection is likely to be triggered. The impact on the restriction of consumers depends on the possibility of importing electricity from foreign power systems.

(29) Dry period

Scenario:

Low water levels cause the hydropower plants to shut down. Pump-storage hydropower plants cannot operate, either. Thermal and nuclear power plants operate under a restricted regime due to the low volumes of cooling water in the tanks. The demand for electricity does not change, but the system gets into deficit.

Scenario evaluation:

Crisis scenario rating	Cross-border dependency rating	Overall rating
Critical	Major	10

Scenario evaluation in words:

The incident would mainly have an impact on the restriction of production and on cross-border transfers; the impact is evaluated as critical. Combined with adverse circumstances, such as planned shutdowns and unscheduled emergency shutdowns, a manual or automatic demand disconnection is likely

to be triggered. The impact on the restriction of consumers depends on the possibility of importing electricity from foreign power systems.

Tab. 2 Summary table of crisis scenario ratings

Crisis scenario rating						
Impact		**Likelyhood**				
EENS	**LOLE**	**Very likely**	**Likely**	**Possible**	**Unlikely**	**Very unlikely**
Disastrous	Disastrous			28 29	27	
Disastrous	Critical			6		
Critical	Disastrous				24	
Disastrous	Major				5	
Major	Disastrous				23	
Disastrous	Minor					
Minor	Disastrous					
Disastrous	Insignificant					
Insignificant	Disastrous					
Critical	Critical					
Critical	Major					
Major	Critical			10		
Critical	Minor					
Minor	Critical					
Critical	Insignificant					
Insignificant	Critical					
Major	Major			16	1 2	
Major	Minor					
Minor	Major				17	
Major	Insignificant					
Insignificant	Major					
Minor	Minor					
Minor	Insignificant					
Insignificant	Minor					
Insignificant	Insignificant					

2.3 Group measures to prevent and resolve emergencies

Group 1	(1) A cyberattack against the critical business ICT infrastructure of the entities connected to the electricity system, such TSOs, DSOs, power plants, and large (industrial) customers (2) A cyberattack against the important business ICT infrastructure in market participants (not physically connected to the electricity system) (6) Insider attack (17) The loss of ICT systems for real-time operation

The application of suitable technical, personnel and organisational measures to ensure cybersecurity has been transposed into the Slovak legislation by Act No. 69/2018 Coll. on cybersecurity and on amendments to certain acts.[3]

[3] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/

Preventive measures

The preventive security measures are implemented pursuant to the provisions of decree No. 362/2018 Coll. of the National Security Authority which lays down the content of security measures, content and structure of security documentation, and scope of general security measures.[4]

An incident is considered serious if identification criteria for the incident of grade 1 (one) category are met, that is:

- the incident restricted or interrupted the operation of an essential service or a critical infrastructure element for more than 15,000 user-hours, where the term 'user-hour' refers to the number of affected users in the territory of at least one district for 60 minutes;
- the incident has caused an economic loss or material damage of more than EUR 250,000 to at least one user.

In the event of a cyberattack, the essential service provider is obliged to:

- immediately notify the competent authority and CERT-SK of any incident having a material effect on the continuity of the essential services provided;
- handle the cybersecurity incident;
- cooperate with the National Security Authority and CERT-SK in handling the reported cybersecurity incident and provide them with the necessary assistance;
- cooperate with law enforcement authorities.

A response to the cybersecurity incident is managed by a SK-CERT unit which, with the participation of the essential service provider, carries out:

- detection of cybersecurity incidents;
- response, delimitation, solution and correction of the consequences of cybersecurity incidents;
- assistance with the handling of the cybersecurity incident on site;
- reaction to the cybersecurity incident;
- support to the reactions to cybersecurity incidents;
- coordination of the reactions to cybersecurity incidents;
- measures designed to prevent further continuation, spread and recurrence of cybersecurity incidents;
- an analysis of cybersecurity incidents.

Crisis situation:

An attack against computer systems of the entities operating in the electricity sector may disable the control of system elements and/or shut them down which may even result in triggering an automatic demand disconnection and interruption of cross-border electricity exchanges. With respect to addressing similar crisis situations, the TSO has internal regulations in place to restore the operation of key facilities (e.g., a business continuity plan pursuant to Commission regulation (EU) 2017/1485 establishing a guideline on electricity transmission system operation (hereinafter only referred to as the "SOGL"). The regulations are not available to the public.

Group 2	(5) Threat to key employees (23) Strike, riots, industrial action

Strikes are usually associated with a complete or partial disruption of work performed by employees which results in the restriction of the operation of an entity or facility.

[4] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/362/

Under certain circumstances it may escalate into physical attacks (sabotage) that may target the affected company and its management and key employees. These employees often have access to facilities that are capable of triggering a crisis situation. The term facilities in this context means not only software and hardware, but technological facilities as well.

The employees' right to strike is guaranteed by the Constitution of the Slovak Republic. A relevant trade union body is competent to announce the strike and decide on its commencement. The competent trade union body is required by law to notify the strike to the employer in writing at least three working days prior to its commencement.

The competent trade union body is required to provide to the employer in writing, at least two working days prior to the commencement of the strike, any strike-related information that is known to it that may help the employer to introduce work schedules to ensure that the necessary operations and services are maintained during the strike. The necessary operation and necessary services are such operations and services the disruption or discontinuance of which poses a threat to life and health of employees or other persons and causes damage to such machinery, facilities and devices whose nature and purpose do not allow for disrupting or discontinuing their operation during the strike.

Preventive measures:
Preventive measures are activated if, even after negotiations with the competent trade union body, no mutual agreement has been reached and the trade union body refuses to cancel or postpone the strike.

In order to keep the employees on strike, protesters, and other unauthorised persons away from the premises designed for key employees, the TSO and RDSO control rooms have internal regulations in place. For such cases, the TSO has also internal regulations in place to restore the operation of key facilities (the business continuity plan pursuant to the SOGL).

Crisis situation:
If, despite the preventive measures having been implemented, a deliberate intervention by an attacker in a key facility occurs and the electricity system exceeds the criteria for the declaration of electricity emergency, the TSO or DSO proceeds in accordance with the system defence plan against the spread of failures the aim of which is to restrict the occurrence of major system failures though early interventions in the system.

If the failure keeps spreading despite the measures adopted:

- TSO will request a cross-border assistance under the contracts between TSOs;
- TSO will request an emergency assistance beyond the framework of valid emergency assistance contracts;
- TSO will initiate a manual demand disconnection procedure.

Group 3	(10) Cold spell (16) Multiple failures caused by extreme weather (28) Heatwave (29) Dry period

Extreme weather conditions such as high temperatures, droughts or cold spells have a negative impact on the operation of generation sources which may result in the lack of sources leading to restrictions in electricity supply. Electricity transmission and distribution facilities are especially at risk, whose failure may lead to local outages in electricity supply with a potential for the further spread of the failure.

Preventive measures:

The preventive measures in connection with scenarios 10, 16, 28 and 29 are activated in the event of a long-lasting period of extreme weather where some of the extreme weather conditions is forecast to further continue with a sufficient degree of probability. Due to the situation being critical already, the transmission facilities are running at their operational limits and basic security criterion N-1 is not complied with.

- The TSO will adjust the schedule of planned shutdowns and downtimes of facilities and review the performance of operations that are essential;
- The TSO intensifies communication with producers and DSOs;
- The TSO and DSOs notify external suppliers and co-workers of potential hazard;
- The TSO and DSOs consider the options of deploying available personnel in the crisis area;
- When planning the operations, the TSO considers possible risks, optimises the plan of operation of generation sources, and plans the operation of hydropower plants in order to optimise levels in water reservoirs and in reservoirs of pumped-storage hydropower plants;
- The TSO communicates with the Slovak Water Management Company (*Slovenský vodohospodársky podnik*) and the Slovak Hydrometeorological Institute (*Slovenský hydrometeorologický ústav*) to monitor hydrological and meteorological developments;
- The TSO carries out weekly assessment of the adequacy of sources in order to identify risks related to the source adequacy;
- The TSO informs the MoE well in advance of the risk of occurrence of crisis situation and, subsequently, regularly communicates with the MoE about its development;
- The TSO and the MoE provide information about the activation of preventive measures on their websites;
- The TSO communicates with neighbouring TSOs about the possibility of electricity supply.

Crisis situation:

A crisis in electricity supply caused by extreme weather conditions carries a risk of serious and long-term interruption of electricity supply to customers and requires special coordination among all stakeholders. If the incident results in an unexpected power imbalance, a Slovak Electricity Operation Centre (*Slovenský elektroenergetický dispečing* (SED)) operator considers the options to address the situation and carries out measures aimed at:

- mobilising electricity generation facilities in the Slovak electricity system pursuant to contracts on the provision of relevant ancillary services;
- operative import of regulatory electricity from other transmission systems pursuant to the Energy Sector Act, the TSO Technical Conditions, the Rules of Operation of the Transmission System Operator;
- regulating electricity consumption;
- changing network configuration;
- if the system overload cannot be resolved through aforementioned measures, the SED has a right to change the structure of connection of the generation facilities of an electricity producer in the necessary extent.

If, during the breakdown of the Slovak electricity system, the connection between individual control rooms is lost, the respective control room operators proceed in accordance with a relevant operational instruction in order to create the largest possible, power balanced, synchronously working parts of the systems pursuant to the foregoing paragraphs of this chapter. Once the connection has been restored, the cooperating control room operators exchange information on the measures implemented.

Group 4	(27) Pandemic

The pandemic puts at risk regular operation of the companies in the electricity sector. The lack of healthy technical personnel may lead to reduction of electricity generation or downtimes which may in turn result in the lack of sources and inability to supply contracted volumes of electricity. The lack of control room operators and other specific positions that cannot be substituted may disrupt the TSO's and DSOs' capacity to reliably control Slovakia's electricity system.

Preventive measures:

Preventive measures related to scenario 27 are activated if the Public Health Authority of the Slovak Republic issues a warning of the occurrence of pandemic situation. If the number of electricity market participants affected by the pandemic is expected to be so high that it may threaten not only their operation but also the stability of the electricity system, the TSO, RDSOs and major network users adopt the following measures:

- work from home;
- restrictions on business travels, physical meetings and workshops that are not essential for business operation;
- restrictions or postponement of maintenance works unless necessary;
- more stringent hygienic requirements and regular inspection of their compliance in the workplace;
- compliance with the general instructions of the Public Health Authority of the Slovak Republic for the prevention of the spread of contagious disease;
- preparation of internal procedures for crisis situations related to the infectious disease which are supplemented and amended in response to the most recent development and experience;
- special regime set for key employees in order to maximise their protection;
- measures implemented in accordance with recommendations of the government/chief hygienist's office/Public Health Authority.

The TSO regularly monitors the capability of producers, customers and system operator to perform their tasks and obligations with respect to supply of electricity.

Specific measures applicable to TSO and DSO control rooms:

- access to control rooms is only allowed for operators and personnel necessary for the operation of the control room;
- operators' body temperature is measured upon entry to the control room;
- direct contact between individual shifts of control room operators is avoided;
- a system operator must have a back-up control room activated if any of the operators contracts the infection;
- the control rooms are disinfected prior to the arrival of a new shift.

Crisis situation:

A crisis situation occurs if a significant portion of entities participating in the stable operation of the electricity system is unable to carry out their regular activities and ensure uninterrupted operation. If the incident results in an unexpected power imbalance, a SED operator considers the options to address the situation and carries out measures aimed at:

- mobilising the remaining available electricity generation facilities in the Slovak electricity system pursuant to contracts on the provision of relevant ancillary services;
- operative import of regulatory electricity from other transmission systems pursuant to the Energy Sector Act, the TSO Technical Conditions, the Rules of Operation of the Transmission System Operator;

- regulating electricity consumption;
- changing network configuration;
- if the system overload cannot be resolved through aforementioned measures, the SED has a right to change the structure of connection of the generation facilities of an electricity producer in the necessary extent.

Group 5	(24) Industrial/nuclear accident

A leak of hazardous substance may endanger life, health or property and may lead to a partial or complete shutdown of a generation facility. In the case of a failure on a nuclear facility, actions are taken pursuant to concrete emergency plans of that facility prepared in compliance with Slovak and EU legislative requirements.

Decree No. 55/2006 of the Nuclear Regulatory Authority of the Slovak Republic on the details of emergency planning for incidents or accidents[5] defines 3 classification grades of incidents or accidents based on which the subsequent measures are adopted.

Grade 1 „alert"– there is a risk of radioactive leak or radioactive substances have leaked already, which may result in the leakage of radioactive substances outside the building structures of the nuclear facility in the case of adverse event development.

- competent emergency response units in the territory of the nuclear facility are notified and alerted and, if necessary, persons in charge of civilian protection under a civilian protection plan, as well. Internal Emergency Plan measures are implemented.

Grade 2 "emergency in the territory of the nuclear facility" – the situation may escalate, or has escalated, into a leakage of radioactive substances outside the building structures of the nuclear facility and to its territory.

- the emergency response unit in the territory of the nuclear facility is alerted and persons in charge of civilian protection under a civilian protection plan are notified, and the warning of civilians is prepared. Internal Emergency Plan measures are implemented.

Grade 3 "emergency in the surrounding of the nuclear facility" – the situation may escalate, or has escalated, into a severe leakage of radioactive substances to the surrounding of the nuclear facility.

- the emergency response unit in the territory of the nuclear facility is alerted and persons in charge of civilian protection under a civilian protection plan are notified, external emergency response forces are alerted in accordance with the Civilian Protection Plan, and the population at risk is warned and informed. Measures arising from the Internal Emergency Plan and the Civilian Protection Plan are introduced and implemented.

The performance and feasibility of emergency planning measures are documented in detail in a preliminary internal emergency plan (applies to the Mochovce 3,4 nuclear power plant) and in internal emergency plans (applies to the Bohunice V2 and Mochovce 1,2 nuclear power plants). Civilian Protection Plans are in place for the areas at risk.

The internal emergency plan applies to incidents or accidents on a nuclear facility that may occur during its operation, and to management of incidents or accidents on other nuclear installations on the site of incident or accident that may occur due a combination of various extraordinary events. The internal emergency plan defines the responsibilities for the performance of measures within the organisational structure of an authorisation holder by establishing an emergency response organisation.

[5] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2006/55/

Preventive measures:

- a regular internal emergency plan exercise with the units defined in the Civilian Protection Plan performed once in three years;
- the units of the authorisation holder's emergency response organisation carry out professional training, exercises or drills at least twice a year;
- a drill involving the entire emergency response organisation of the authorisation holder is performed at least once a year.

Crisis situation

The activation of the reactor protection system shuts down the reactor in the case of abnormal operation. Once the cause of the activation of the reactor protection system is removed, the block's operation may resume after the verification that its restoration is safe.

Under emergency conditions, the reactor is shut down by the system of reactor safeguards triggered after the activation of "safety assurance system" signals. The block's operation is prohibited under emergency circumstances. The reactor must be put in a safe condition.

The public is notified of a radiation event with possible environmental impacts by means of a siren warning system, complemented with the spoken information. More detailed information about the possible hazard is provided through municipal PA systems or nation-wide public TV and radio broadcast.

Protection of employees who cannot quit their work and are present in the area at risk is ensured through:

- individual protection by means of personal protective equipment;
- moving employees to a radiation shelter;
- adjusting the work regime, rest and rotation of employees in a shift.

If the affected nuclear facility can no longer be operated:

- TSO will request a cross-border assistance under the contracts between TSOs;
- TSO will request an emergency assistance beyond the framework of valid emergency assistance contracts;
- TSO will initiate a manual demand disconnection procedure.

In the event of a synchronous system breakdown, after the restoration of frequency following a frequency deviation exceeding ±200 mHz, and when restoring the operation of the Slovak electricity system after a "black-out" event or failure, the TSO proceeds in line with the measures in the Defence Plan and the Restoration Plan After System Breakdown.

3. ROLES AND RESPONSIBILITIES OF COMPETENT AUTHORITIES

3.1 Competent authorities and bodies to which tasks have been delegated in the case of emergency in the electricity sector

Ministry of Economy of the Slovak Republic

The roles and responsibilities of the MoE as the competent authority are laid down in Act No. 251/2012 Coll. on the energy sector[6] (hereinafter only referred to as the "Energy Sector Act"). Pursuant to the provisions of the Energy Sector Act, the MoE ensures the monitoring of compliance with security of electricity supply requirements, adopts measures for the security of electricity supply, and decides on the implementation of measures where the integrity of the system and network or the secure and reliable operation of the system and network are at risk. The MoE publishes an annual report on the monitoring of security of electricity supply for the previous year.

The MoE carries out the roles of a secretariat of the Energy Security Committee which, under Act No. 110/2004 Coll. on the functioning of the Security Council of the Slovak Republic at the time of peace[7], evaluates the security situation. The MoE sends immediately, at least once a month, a report on the results of the evaluation to the Office of the Security Council of the Slovak Republic. The MoE draws up proposals for the Security Council of the Slovak Republic for mitigation or elimination of risks in the energy sector.

In the event of an electricity crisis, the MoE, upon consultations with the transmission system operator, declares the electricity crisis and immediately informs competent authorities of the Member States within the same region and the Commission to that effect. The MoE provides information about the causes of the crisis, the measures planned and adopted to mitigate the crisis, and on a possible need of assistance from other Member States. Within three months of the end of the electricity crisis, the MoE reviews the crisis and its consequences.

If a seasonal adequacy assessment or other qualified sources indicate specific, serious, and reliable information that an electricity crisis may occur, the MoE issues an early warning to the Commission and competent authorities of the Member States within the same region without undue delay. The MoE also provides information about the causes of the possible electricity crisis and about the measures planned or adopted to prevent the crisis, and on a possible need of assistance from other Member States.

The Security Council of the Slovak Republic and the Energy Security Committee of the Slovak Republic

The Security Council of the Slovak Republic is involved in the coordination of planning, preparatory and implementing measures in the area of security of the Slovak Republic. It assesses the proposals for security measures submitted by the ministries, other central government bodies, other general and local government bodies, and committees of the Security Council of the Slovak Republic, and submits its opinions on such proposals to the Slovak government.

The Energy Security Committee communicates and cooperates with other bodies and institutions within the Security Council of the Slovak Republic; its chairman convenes a meeting of the committee members in the event of an imminent electricity crisis.

Transmission system operator

In direct connection with the occurrence of emergency, or in the case of activities that immediately prevent its occurrence, or in the event of malfunctions of system installations and during their removal, the TSO has a right to restrict or suspend the transmission of electricity in the necessary extent and for the necessary period of time. The TSO declares and revokes an electricity emergency within the

[6] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2012/251/

[7] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/110/20160101

defined territory or its part. For these purposes, the TSO prepares, in cooperation with affected energy business entities, a defence plan against the spread of failures and a restoration plan after system breakdown, which define the measures designed to prevent the spread of failures in the Slovak electricity system, as well as the measures to restore electricity transmission and distribution after a system breakdown. Individual measures are subject to real-life testing (where a measure can actually be tested during the real-life operation) in such extent and under such conditions as not to threat the security of the system's operation.

Distribution system operator

Pursuant to the Energy Sector Act, a DSO has a right to request the TSO to declare a state of emergency in the part of the defined territory (a territory or its part controlled by a particular DSO). Once the emergency has been declared in the part of the defined territory, the DSO has a right to restrict or suspend the distribution of electricity in the necessary scope and for the necessary period of time. Upon the TSO's control room's instruction, the DSO's control room is required to declare restrictive electricity emergency measures and specify measures designed to eliminate the emergency. In line with the hierarchy of the dispatching management, the TSO's control room serves as the main coordinator in electricity emergencies.

3.2 Competent authorities and bodies to which critical infrastructure related tasks have been delegated

The powers and a complete list of responsibilities of competent authorities in charge of critical infrastructure are laid down in Act No. 45/2011 Coll. on critical infrastructure[8]

Government of the Slovak Republic

The Slovak government approves a critical infrastructure concept, defining the objectives, priorities and their implementation, for a relevant period. The government is responsible for the specification of sectoral and cross-sectoral criteria and decides on the determination of an element and its inclusion to a sector.

Ministry of the Interior of the Slovak Republic

The ministry coordinates the performance of central government bodies in terms of critical infrastructure. Within the scope of its powers, it defines the scope of sensitive information and persons eligible to access sensitive information. The role of the ministry is to oversee, in cooperation with a competent central government body, the compliance with the responsibilities of an operator of a European critical infrastructure element, and serves as a contact point for the protection of the elements of the European critical infrastructure.

Ministries

The ministries are central government bodies. In cooperation with the Ministry of the Interior of the Slovak Republic, they prepare and update a sector risk analysis with respect to the critical infrastructure. In cooperation with a critical infrastructure element operator, they define the scope of sensitive information and designate a person eligible to access such sensitive information. The central government bodies are also obliged to inspect the fulfilment of operator's responsibilities and to submit a summary report from the operators' inspection to the Ministry of the Interior of the Slovak Republic.

Critical infrastructure element operator

The role of the operator is to protect the critical infrastructure element against its disruption or destruction. The operator must have a security plan or an emergency plan (applies to operators under a separate regulation) in place. The security plan should contain a description of possible disruptions

[8] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/45/20210301.html

or destruction of the element, element's vulnerabilities, and security measures for its protection; the plan must be regularly reviewed and tested at least once in three years in a model situation of element's disruption or destruction.

Operators of undertakings with the presence of a dangerous substance are subject to the provisions of Act No. 128/2015 Coll. on prevention of serious industrial accidents[9]. Pursuant to said act, each operator is obliged to:

- adopt measures to prevent serious industrial accidents and to mitigate their effects on human health, the environment, and property;
- carry out a serious industrial accident risk assessment and implement a system to assess and manage the risk of a serious industrial accident related to the undertaking's operation, including a monitoring and control system;
- draw up a programme to prevent serious industrial accidents and ensure its implementation;
- ensure the public is informed;
- report serious and other industrial accidents.

In addition, category B undertakings, that is, undertakings that meet the conditions under §3(3) of Act No. 128/2015 Coll., are also obliged to:

- draw up a security report;
- draw up an internal emergency plan;
- submit documents for a civilian protection plan;
- ensure that a rapid and effective serious industrial accident response service is available, equipped with the necessary organisational, material and personnel resources;
- ensure the financial coverage of liability for damage.

3.3 Competent authorities and bodies to which cybersecurity tasks have been delegated

The organisation, powers and responsibilities of public authorities and the responsibilities of providers of essential services and providers of digital services in the field of cybersecurity are laid down in Act No. 69/2018 Coll. on cybersecurity and on amendments to certain acts[10].

National Security Authority (hereinafter only referred to as the "NSA")

The NSA manages and coordinates cybersecurity actions at the general government level and serves as a national CSIRT unit. Its role is to provide methodology guidelines for the preparation of operational procedures to respond to cyber threats at the national level. The NSA cooperates with security analytical units in order to exchange and share information about security incidents.

General government bodies provide the NSA with the necessary assistance and essential information they obtain in order to ensure cybersecurity.

With respect to preventing cybersecurity incidents, the NSA regularly monitors the national cyberspace and analyses potential and current threats. As part of Slovakia's crisis management system, it proposes and draws up a response procedure to cyberattacks and determines incident-handling principles. It also provides guidelines for incident response units and oversees their operations.

In the event of a serious cybersecurity incident or a threat thereof, the NSA may:

- alert and warn of a serious cybersecurity incident;
- impose an obligation to carry out a reactive measure;

[9] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2015/128/
[10] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/

- request a proposal of measures and implementation of measures designed to prevent further continuation, spread and recurrence of a serious cybersecurity incident.

Essential service provider

An essential service provider is obliged to adopt and comply with general security measures related to tasks, processes, roles and technologies in the organisational, personnel and technical area, whose aim is to ensure cybersecurity throughout the lifetime of networks and information systems.

The essential service providers is obliged to report each serious cybersecurity incident it has identified on the basis of the criteria set for individual categories of cybersecurity incidents.

The essential service provider is further obliged to:

- handle a cybersecurity incident;
- immediately report any serious cybersecurity incident;
- cooperate with the NSA and a central government body in handling the reported cybersecurity incident and provide them with the necessary assistance for this purpose, as well as any information it has obtained through its own activities that is relevant to the handling of the cybersecurity incident;
- at the time of the cybersecurity incident, to preserve evidence or a means of evidence that can be used in criminal proceedings;
- report to a law enforcement authority or the Police Corps the facts indicating that a cybersecurity incident-related crime has been committed if it has learnt of such crime in a credible manner.

The essential service provider is obliged to immediately report and prove to the NSA through an integrated cybersecurity information system that a reactive measure has been carried out, and its outcome.

Digital service provider

A digital service provider is obliged to adopt and comply with appropriate and adequate security measures (pursuant to a separate regulation) in order to manage the risks associated with a threat to the continuity of a digital service and cybersecurity incident-handling process. For this purpose, the digital service provider is obliged to allocate sufficient personnel, material, technical, time and financial resources in order to ensure the continuity of the digital service.

The digital service provider is further obliged to:

- report any cybersecurity incident if it has information at its disposal based on which it is capable of identifying whether that cybersecurity incident has a material effect as defined in a separate regulation, immediately after it has learnt of the incident;
- handle the reported cybersecurity incident;
- cooperate with the NSA in the handling of the reported cybersecurity incident.

The digital service provider is obliged to immediately report and prove to the NSA through an integrated cybersecurity information system that a reactive measure has been carried out, and its outcome.

4. NATIONAL PROCEDURES AND MEASURES

4.1 Electricity emergency

A sudden or impending electricity shortage, a change in the system frequency above or below the level set for technical means ensuring automatic disconnection of facilities from the system in compliance with the technical conditions of the transmission system operator or a disruption in the parallel operation of transmission systems which may cause a considerable reduction or interruption of energy supply or put energy facilities out of operation or endanger the life and health of people are defined in the national legislation as a "**state of emergency in the electricity sector (electricity emergency)**" (§20 of the Energy Act[11]). State of emergency may be declared as a result of:

a) an extraordinary event or a crisis situation;
b) measures of economic mobilisation;
c) accidents in electricity generation, transmission and distribution facilities, even outside the defined territory;
d) a threat to the safety and reliability of the system operation;
e) an imbalance in the system or its part;
f) a terrorist offence.

Figure 1 Procedure for declaring a state of emergency in the electricity sector

Occurrence of an incident having an impact on the supply of electricity	
TSO	• evaluation of the situation by the TSO's dispatcher • where the conditions for the declaration of a "state of emergency in the electricity sector" are met, the responsible persons of the TSO are notified
TSO	• based on information from the control room operator, the situation is assessed by the TSO's responsible persons • an authorised senior employee notifies the control room operator of the decision to declare electricity emergency
TSO	• the request to broadcast an announcement concerning the declaration of electricity emergency is communicated by the control room operator to the designated persons of selected public service mass media
Public service mass media	• confirmation of the receipt of announcements concerning the declaration of electricity emergency by designated employees of selected public service mass media
Public service mass media	• the announcement is broadcast in the public service mass media in accordance with the agreed conditions pursuant to the Methodology for Ensuring Radio and Television Broadcasting during a State of Emergency in the Electricity Sector
TSO	• TSO's control room operator informs the control rooms of DSOs and operational staff of customers and generators directly connected to the transmission system about the declaration of electricity emergency
TSO / MoE	• TSO's control room operator informs the Economy Ministry about the declaration of electricity emergency, completes and sends the initial report on the declaration of electricity emergency to the MoE • after obtaining additional information, the operator will send, upon request, a more detailed report on the declaration of electricity emergency

[11] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2012/251/

Electricity emergency is declared and revoked by the TSO's control room through public service mass media and by using the means of dispatching management. The declaration and revocation of an electricity emergency must be notified by the TSO to electricity customers and generators connected to the transmission system, the DSOs' control rooms and to the MoE. In the event of an electricity crisis at the DSO level, emergency state is declared and revoked by the TSO's control room based on a request received from the DSO's control room.

Electricity emergency is declared prior to the adoption of restrictive measures. In the event of a major incident, such as system breakdown or impending system breakdown, electricity emergency may be declared subsequently; however, without any delay after adopting the measures necessary for the protection and restoration of the system.

The declaration of an electricity emergency, blackout and restoration state shall be communicated by the TSO of the Slovak Republic to the neighbouring TSOs and other relevant entities, such as defence service providers, the nominated electricity market operator (Organizátor krátkodobého trhu s elektrinou/short-term electricity market operator, hereinafter referred to as "OKTE"), the relevant regulatory authority (Regulatory Office for Network Industries; hereinafter referred to as "RONI") and other entities as necessary.

The MoE sends immediately, at least once a month, a report on the results of the evaluation to the Office of the Security Council of the Slovak Republic.

4.2 Preventive measures in the electricity sector

Report on the monitoring of security of electricity supply

The report is a document prepared by the MoE based on documentation provided by the TSO. It contains the evaluation of development and the balance of electricity consumption and generation, the structure of source base, projection of electricity supply development for the next five years and the prospects for the security of electricity supply for the period between five and 15 years, development intentions of the transmission system operator, ensuring the safety and reliability of Slovakia's electricity grid, including measures to cover peak demand and handle outages, transmission quality and maintenance of the system.

Climate Change Adaptation Strategy of the Slovak Republic

The Climate Change Adaptation Strategy of the Slovak Republic[12] (hereinafter referred to as the "Strategy") brings a systemic approach towards setting up interim and planned measures to be introduced with a view to minimising losses, damage and economic costs associated with the climate change. In the energy sector, Slovakia's goal is to build a competitive low-carbon energy industry which will ensure a secure, reliable and effective supply of all forms of energy at reasonable prices while taking into account the protection of customers and sustainable development. The strategy evaluates potential risks caused by climate change and proposes a set of managerial, technical, technological and structural adaptation measures for the energy sector:

- modelling the climate impact on existing and planned assets;
- cooperation with meteorological services and forecasting with the use of climate information;
- evaluation of hydrological data and simulations of possible events for hydroelectric plants and process water;
- in order to address the challenge of water scarcity: the recycling of water, the use of rainwater or urban waste water;
- international cooperation and coordination of joint course of action;

[12] https://www.minzp.sk/files/odbor-politiky-zmeny-klimy/strategia-adaptacie-sr-zmenu-klimy-aktualizacia.pdf

- increasing the interconnection of systems;
- decentralising electricity generation;
- promoting cost-effective measures as regards energy efficiency in the Slovak Republic for the purposes of reducing energy consumption.

National Cyber Security Strategy 2021 – 2025

The National Cyber Security Strategy[13] is the key strategic document comprehensively determining Slovakia's strategic approach to ensuring cybersecurity. The document contains a comprehensive concept for the management of information security and cybersecurity. It reflects Slovakia's strategic direction in terms of security, taking into account the principles of the Security Strategy of the Slovak Republic while also drawing from the strategic documents of NATO, the EU, the OECD and the UN. The document also identifies weak points in Slovakia's cybersecurity and describes measures to address them with a view to attaining the required target level of security.

Test plan

The test plan represents a practical verification of procedures for the declaration and revocation of a state of emergency or for preventing a state of emergency in the electricity sector. Entities subject to testing include the TSO, DSOs, OKTE, the MoE, significant grid users and selected electricity market participants.

Testing applies to facilities and instruments used when ensuring the declaration and revocation of a state of emergency, communication devices, internal procedures and processes of the entity subjected to testing. Tests are carried out once every five years.

The TSO is designated as an entity authorised to perform the emergency test. The test must be in line with the TSO's technical conditions to the extent necessary for ensuring the security and reliability of system operation.

Defence plan against the spread of failure and restoration plan after system breakdown

The plans are drawn up by the TSO in cooperation with the energy business entities concerned. The TSO defines the measures to prevent the spread of failures in the Slovak electricity system, as well as the measures to restore electricity transmission and distribution after a system breakdown. Individual measures are subject to real-life testing (where a measure can actually be tested during the real-life operation) in such extent and under such conditions as not to threat the security of the system's operation. The foregoing is described in more detail in chapter 4.3.

4.3 Measures to prevent and mitigate the impacts of electricity crises

If preventive and preparatory measures are insufficient, the provisions concerning "the state of emergency in the electricity sector" shall apply. The tasks of electricity market participants and procedures in putting restrictive measures in place are detailed in Ministry of Economy Decree No. 416/2012 Coll. laying down the details on the procedure for the application of restrictive measures in emergency and on measures designed to eliminate emergency in the electricity sector[14] (hereinafter referred to as the "Decree on States of Emergency").

When eliminating a state of emergency, the TSO's or DSO's control room is required to proceed in accordance with the system defence plan against the spread of failures and the restoration plan after system breakdown.

[13] www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Strategia_kybernetickej_bezpecnosti_2021.pdf
[14] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2012/416/

In adopting restrictive measures in the electricity sector, the TSO or DSO shall not go beyond what is necessary for restricting or interrupting the supply of electricity for public utility services and household electricity customers.

All electricity market participants are required to submit to the measures aimed at mitigating an electricity crisis situation, both during their preparation and implementation. Where an electricity emergency has been declared, electricity market participants are required to participate in eliminating the reasons and consequences of the electricity emergency and in restoring the supply of electricity.

Non-market measures, such as a forced disconnection of electricity consumption or delivery of extraordinary supply outside the regular functioning of the market, should also be adopted as the last resort only, after all other possibilities offered by the market have been exhausted. The forced disconnection should only be applied after all possibilities of voluntary disconnection have been exhausted. In addition, all non-market measures should be necessary, proportional, non-discriminator and temporary. The energy businesses and customers should have a possibility to use the market-based mechanisms for as long a time as possible during the solving of electricity crises.

4.3.1 Measures to prevent electricity crisis situations

Under normal operation of Slovakia's electricity grid, the output balance is maintained solely by means of measures that are based on market principles (procurement of regulating reserves /ancillary services, non-guaranteed regulating electricity or emergency assistance from abroad).

In order to prevent an electricity crisis situation or during a state of emergency in the electricity sector or in preventing a state of emergency in the electricity sector, the TSO is authorised to use, in addition to market-based instruments, also non-market technical instruments, such as:

- Restricting the consumption of electricity – implemented through the Consumption Restriction Procedure during electricity shortage in the transmission system and the distribution system. If it is not possible to ensure a sufficient amount of electricity, restriction of electricity consumption by the customers is based on restrictive power offtake levels.
- Interrupting the distribution of electricity – for this purpose, the Demand Disconnection Procedure is applied. The supply of electricity to customers is interrupted by switching off the specific terminals in high and very high voltage substations based on the applicable emergency switch-off level, with possible cyclic alternation in switching off such terminals.
- Changing the amount of power supplied by electricity generator to the system – authorising the system operator to request that electricity generator changes the amount of power it supplies to the system, subject to the technical limits of the source.
- The use of free production capacity – authorising the system operator to request that electricity generator uses all free production capacities for keeping the system stable.
- Operatively switching off a part of the facility to the extent necessary for stabilising the output balance of the affected part of the system – authorising the system operator to switch off some of the facilities to the extent necessary for maintaining a safe and stable system.
- Measures to restore the transmission and distribution of electricity – measures included in the Restoration Plan. This involves a set of technical and organisational procedures and measures facilitating the restoration of normal operation as soon as possible.

The measures to prevent electricity emergencies are described in detail in part 4 of the Technical Conditions of the Transmission System Operator document.[15]

[15] https://www.sepsas.sk/media/4428/dokument-o-tp-ucinnost-jan-2021.pdf

4.3.2 Defence Plan

A system of measures aimed at maintaining a stable operation of Slovakia's electricity grid. It involves a set of technical and organisational procedures and measures that allow for preventing an overrun of operational security limits and the spread of failures; the system can be brought back within the standard operational limits while shortening the duration of the system restoration process.

The Defence Plan against the occurrence and spread of major system failures consists of:

- measures against frequency drop or increase within Slovakia's electricity grid;
- measures against voltage drop or increase;
- measures to prevent overload on elements in the transmission system of the Slovak Republic.

During operational management of the electricity grid in the case of electricity emergencies and temporary shortage of power, the Defence Plan uses the procedures based on:

- the electricity consumption restriction procedure (manual action);
- the demand disconnection procedure (manual action);
- the low frequency demand disconnection (automatic action).

The Defence Plan, its measures and procedures are described in part 2 of the Technical Conditions of the Transmission System Operator document.[16]

4.3.3 Electricity consumption restriction procedure

In Slovakia's electricity grid, the electricity consumption restriction procedure is a restrictive measure in the electricity sector which is applied during shortages of electricity in the transmission and distribution systems whenever the trigger conditions are met. More information about the electricity consumption restriction procedure is provided in Chapter 4.4.1.

4.3.4 Demand disconnection procedure

The demand disconnection procedure is applied by the TSO and DSO during a sudden significant imbalance in the system and when eliminating failures in the transmission or distribution system by interrupting the transmission and distribution of electricity to customers. The supply of electricity to customers is interrupted by the TSO's or DSO's control room by switching off the specific terminals in high and very high voltage substations based on the applicable emergency switch-off level, with possible cyclic alternation in switching off such terminals.

4.3.5 Low frequency demand disconnection (automatic demand disconnection)

When frequency falls to 49 Hz and below, the TSO and DSO, in implementing restrictive measures in the electricity sector, will proceed in accordance with the low frequency demand disconnection which is part of the frequency plan and is applied automatically.

The low frequency demand disconnection is carried out automatically with the use of technical means for disconnecting electricity consumption, placed in the facilities of DSOs and customers connected to the transmission system.

Based on calculation analyses, the low frequency demand disconnection in Slovakia's electricity grid has been set to six frequency levels. The basic technical criteria of the low frequency demand disconnection are defined in the Synchronous Area Framework Agreement (SAFA), because a measure of this type must be coordinated at the level of the entire Continental Europe (CE) synchronous area.

[16] https://www.sepsas.sk/media/4428/dokument-o-tp-ucinnost-jan-2021.pdf

4.3.6 Frequency plan

The frequency plan allows the TSO and DSOs, by early intervention in the operation of the transmission or distribution system following the occurrence of system failures, to restore and maintain the frequency of the system at values where the technical equipment of electricity generators and customers is not at stake, and to create conditions necessary for bringing the frequency back to the normal system frequency range, which means an interval between 49.8 Hz and 50.2 Hz. The frequency plan is activated if the system frequency reaches a threshold of 49.8 Hz or 50.2 Hz.

The principles of the consumption restriction procedure, the demand disconnection procedure and the low frequency demand disconnection are specified in Annex 1 to Ministry of Economy Decree No. 416/2012 Coll. on restrictive measures in emergency.

4.4 Framework for manual disconnection of demand in the system

In the RG-CE ENTSO-E interconnected system, the nominal frequency represents a frequency of 50.0 Hz; the normal frequency range means an interval between 49.8 Hz and 50.2 Hz. Within the normal frequency range, active power is controlled with the use of ancillary services, such as primary, secondary and tertiary regulation of active power.

If the frequency in the RG-CE ENTSO-E interconnected system deviates from the normal frequency range of 49.8 Hz – 50.2 Hz, the system will enter an emergency state which needs to be resolved by extraordinary measures aimed at bringing the frequency back to the normal range. Extraordinary measures are part of the Defence Plan, the purpose of which is to restore and maintain, by early interventions in the system following the occurrence of major system failures, the system frequency at values where the technical equipment of electricity generators and customers is not at stake, and to create conditions necessary for bringing the frequency back to the normal system frequency range.

Frequency range between 50.2 and 50.5 Hz

When the frequency increases to 50.2 Hz and above, measures are primarily taken on the side of electricity generators connected to the affected part of the system. The regulation of active power supplied to the system is ensured on the basis of instructions from the TSO's control room or by an automatic change in the active power of facilities operated by electricity generators.

If the increase in frequency above 50.2 Hz has caused production outages and the frequency still remains above this value, such power outages are not replaced by the TSO’s control room operator. The TSO’s control room operator activates power reserves until the frequency stabilises within this frequency range; subsequently, the TSO’s control room operator proceeds in line with the Restoration Plan.

Frequency range in excess of 50.5 Hz

If the frequency exceeds 50.5 Hz, the TSO’s control room operator gradually activates power reserves. The operator will continue mobilising the reserves until the frequency falls below 50.4 Hz. If the frequency could not be brought back below 50.4 Hz by mobilising the reserves, the TSO’s control room operator is authorised to seek emergency assistance pursuant to applicable emergency assistance contracts with the neighbouring TSOs. After the frequency is brought back below 50.4 Hz, the TSO control room operator will suspend increasing consumption and lowering generation and subsequently proceeds in accordance with the Restoration Plan.

Frequency range between 49.8 and 49.5 Hz

If the frequency is regulated manually, the operator proceeds in a manner that has the least impact on customers in Slovakia's electricity grid. Where the system frequency could not be brought back to the normal range following the automatic activation of measures under the Defence Plan, the TSO’s

control room operator manually activates reserves until the frequency stabilises within this frequency range; subsequently, the TSO's control room operator proceeds in line with the Restoration Plan.

Frequency range between 49 and 49.5 Hz

If the frequency drop could not be stopped and if it continues to fall below 49.5 Hz, the TSO's control room operator gradually activates power reserves. The operator will continue mobilising the reserves until the frequency increases above 49.6 Hz. If the frequency could not be brought back above 49.6 Hz by mobilising the reserves, the TSO's control room operator is authorised to seek emergency assistance pursuant to applicable emergency assistance contracts with the neighbouring TSOs. If emergency assistance has not been provided or if it is insufficient for increasing the frequency above that value, the TSO's control room operator may activate the Consumption Restriction Procedure or the Demand Disconnection Procedure. After the frequency is brought back above 49.6 Hz, the TSO's control room operator will suspend increasing generation and activating the stages under the Consumption Restriction Procedure or the Demand Disconnection Procedure and will subsequently proceed in accordance with the Restoration Plan.

Frequency below 48 Hz

If the frequency falls to 47.5 Hz or below, selected facilities of the electricity generators will be automatically disconnected from the affected part of the system and will be switched to house load operation. The units of electricity generators will be disconnected upon reaching such frequency values that will prevent exceeding the technical limitation of the electricity generators' facilities and ensure a reliable transition to house load operation.

4.4.1 Electricity consumption restriction procedure

In Slovakia's electricity grid, the electricity consumption restriction procedure is a restrictive measure in the electricity sector which is applied during shortages of electricity in the transmission and distribution systems whenever the trigger conditions are met.

The electricity consumption restriction procedure determines the restriction of customers' electricity consumption on the basis of restrictive power offtake levels. The individual restrictive power offtake levels may be applied simultaneously. The restrictive power offtake levels are declared and revoked by the TSO's control room within the defined territory through public service mass media and subsequently communicated to customers connected to the transmission system and to the control rooms of DSOs.

Restrictive power offtake levels under the electricity consumption restriction procedure are not applied where the customer is:

- a health facility included in the public minimum network of healthcare providers;
- premises of an emergency medical service, a pharmacy or a provider of medical aids;
- defence infrastructure facility;
- airport or a ground-based aviation facility;
- a building or a facility of the Government of the Slovak Republic, the Ministry of the Interior of the Slovak Republic, the Ministry of Justice of the Slovak Republic, the Police Corps, the Fire and Rescue Service and the Mountain Rescue Service;
- communication and information infrastructure of the integrated rescue system;
- a nuclear facility;
- a facility specified in the economic mobilisation crisis plan;
- an element of critical infrastructure or an element of European critical infrastructure.

Electricity consumption of customers is restricted on the basis of the electricity consumption restriction procedure laid down in the Decree on States of Emergency.

4.4.2 Restoration plan

The Restoration Plan is a system of measures for a gradual restoration of the operation of synchronously interconnected systems. This involves a set of technical and organisational procedures and measures facilitating the restoration of normal operation as soon as possible. DSOs and operators of system facilities for electricity generation in the territory of the Slovak Republic are required to incorporate the Restoration Plan in their internal procedures. The Restoration Plan contains the procedures for handling such electricity grid states as:

- synchronous system breakdown;
- frequency restoration of more than ±200 mHz;
- restoration of the electricity grid operation following the occurrence of an extraordinary event.

The Restoration Plan, its measures and procedures are described in part 3 of the Technical Conditions of the Transmission System Operator document.[17]

4.5 Market activities which can be partially or fully suspended

PPS reserves the right to suspend the market activities if there is a situation in the power system of SR which does not allow to continue the given market activity or in which the given market activity reduces the efficiency of the process of maintaining and/or restoring the normal state (normal state or alert state as defined in SO GL) or the tools and means of communication necessary for carrying out of the market activities are not available.

The list of the mentioned activities is derived from the list defined in NC ER supplemented by the recommendations for implementation of NC ER prepared by ENTSO-E after their adjustments to the conditions of the power system of SR.
Market activities which can be partially or fully suspended:

- Allocation of cross-border capacities in the relevant timeframes according to the relevant auction/allocation rules and the Operational Procedures of SEPS.
- Use of the allocated cross-border capacities on the relevant bidding zone borders.
- Standard processes of the operational planning, procurement of ancillary services (hereinafter referred to as “AnS”) and activation of balancing energy:
    I) daily purchase of AnS,
    II) daily operational planning of AnS,
    III) modification of the daily operational planning of AnS,
    IV) activation process of balancing energy:
        a. from the units providing AnS, e-GCC,
        b. Emergency cross-border exchange of balancing energy,
        c. non-guaranteed balancing energy.
- Provision of a balance position and change of the balance position by the balance responsible parties – provision of daily diagrams of the balance responsible parties.
- Day-ahead trading including all relevant market activities.
- Intraday trading including all relevant market activities.
- Standard evaluation of activated AnS and of balancing energy.
  Standard processes of imbalance settlement and balancing energy settlement.

4.6 Mechanisms for informing the public

Following an assessment of consequences, the TSO declares and revokes an electricity emergency within the defined territory or its part through public-service mass media and by using the means of dispatching

[17] https://www.sepsas.sk/media/4428/dokument-o-tp-ucinnost-jan-2021.pdf

management. The role of public service mass media is fulfilled by the Radio and Television Slovakia (Rozhlas a televízia Slovenska), the SITA Slovak News Agency and the News Agency of the Slovak Republic.

The public must be informed about the declaration of electricity emergency, the declaration of restricted electricity consumption and the declaration of interrupted supply of electricity no later than within 30 minutes of receiving the TSO's request to broadcast the announcement and, subsequently, all throughout the day until the adopted measures are revoked. The TSO informs significant grid users as well as state authorities separately. The TSO's website and trading system are also used as a platform for providing information.

5. REGIONAL AND BILATERAL PROCEDURES

5.1 Cooperation and coordination mechanisms within the region

The TSO has signed bilateral operating contracts and emergency assistance contracts with the neighbouring TSOs. An operating contract between the directly interconnected neighbouring TSOs covers the standard operation, emergency and restoration states.

The contract includes technical parameters and settings for primary and secondary technology, topology connection of substations and facilities with a direct impact on the neighbouring TSO. The contract also contains a list of responsible persons who are in contact with the dispatching management. Operating contracts also cover assistance during crisis situations, in particular during restoration of the system. The limits for the quantities of electricity offered for restoration purposes and potentially usable routes /connections of facilities are defined as well.

Emergency assistance contracts are agreed between the directly interconnected neighbouring TSOs. The agreed emergency assistance is guaranteed on both sides and the supplied electricity is compensated for in a manner agreed in the contract. Operators of neighbouring transmission systems may also agree on non-guaranteed supply of regulating electricity.

5.2 Regional and bilateral measures

The existing regional and bilateral measures applied at the TSO level are described in Chapter 1.2. With respect to the regional measures and cooperation in resolving crisis situations that go beyond the existing contracts between TSOs, Slovakia is engaged in negotiations to define the roles and responsibilities of Member States' competent authorities pursuant to the provisions of the Risk-preparedness Regulation. The common platform established for this purpose includes competent authorities from Austria, the Czech Republic, Germany, Poland, and Slovakia.

The first step to establish the framework for regional cooperation in risk preparedness is to conclude a Memorandum of Understanding on risk-preparedness in the electricity sector (hereinafter only referred to as the "MoU") that will lay grounds for more intensive cooperation and coordination in:

- exchange of information on the security situation and the functioning of crisis management policies with respect to supply of electricity;
- sharing of information on electricity crisis;
- cooperation in the event of electricity crisis;
- testing electricity emergencies.

The Member States participating in the common platform have expressed interest in cooperation in the electricity sector in order to prevent electricity crises, prepare for them and manage them in the spirit of solidarity and transparency, fully respect the requirements of competitive internal market in electricity and the operational security procedures of TSOs, including concurrent crisis situation extending beyond the borders of a single state.

The Member States will cooperate to mutually coordinate regional measures that should be implemented in the event of a crisis and prepare for situations that cannot be resolved by means of market-based measures.

The wording of the MoU is currently being finalised and is expected to be signed at the start of 2022.

5.3 Mechanisms to cooperate and coordinate actions before and during the electricity crisis within the region

Cooperation is coordinated on the basis of standard bilateral operating contracts and the Continental Europe Synchronous Area Framework Agreement (SAFA).

In order to ensure a stable operation of a synchronous area, security coordination centres have been set up on the basis of legislative requirements and their powers include compliance with the operational security limits, monitoring the sufficiency of the source base and ensuring coordination in switching off the facilities.

If the mechanisms described above are insufficient, there are also other procedures available for ensuring an uninterrupted supply of electricity. The procedures fall within the remit of coordination centres and are as follows:

- Extraordinary procedure for frequency monitoring and countermeasures in case of large steady-state frequency deviations (100/50 mHz procedure).
- Additional supplementing procedure for activation of reserves for delayed retrofit TSOs ("Additional delayed retrofit reserves").
- Extraordinary procedure for frequency monitoring and countermeasures in case of long lasting steady-state frequency deviations (grid time deviations)

5.4 Crisis coordinator

The role of crisis coordinator is fulfilled by the TSO which, during an electricity crisis situation, acts in line with the procedures applicable to the state of emergency in the electricity sector.

Contacts to responsible persons:

Transmission system operator **-** **Slovenská elektrizačná prenosová sústava, a.s.**	**Name:**	Ing. Martin Jedinák PhD.
	Position:	head of electricity system operation preparation department
	Phone:	+421 917 177 086
	Email:	martin.jedinak@sepsas.sk

Competent authority **-** **Ministry of Economy of the Slovak Republic**	**Name:**	Mgr. Martin Pitorák
	Position:	director of fuel and energy sector department
	Phone:	+421 2 4854 1911
	Email:	martin.pitorak@mhsr.sk

No crisis coordinator as per the requirement arising from the Regulation has been designated. The Slovak Republic will supplement information about the electricity crisis coordinator after such coordinator has been designated.

6. STAKEHOLDER CONSULTATIONS

The course of consultations with RONI and relevant electricity market participants as regards the selection of national crisis scenarios are described in Chapter 2.1.

Consultations on the draft Preparedness Plan took place on 26.5. - 2.6.2021. The draft Plan was consulted with the relevant electricity market participants and RONI. Participating entities did not use the option of bilateral negotiations with the MoE. The MoE did not receive any key comments on the draft of Risk-preparedness Plan during the consultation. Comments and suggestions for amendments sent by individual entities were taken into account to the extent possible.

Consultations regarding the final draft of the Risk-preparedness Plan, the notification obligation of which is set in Article 10(8) of the Risk-preparedness Regulation, were carried out between 16 November and 1 December 2021. The consultations involved the stakeholders which have participated in the preparation of the Risk-preparedness Plan as working group members through all its stages so far. All stakeholders' comments were resolved bilaterally.

7. EMERGENCY TESTS

Based on Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration, the so-called Test Plan was publicly consulted and approved by the competent authority. The Test Plan is publicly available in the Technical Conditions for Access and Connection and in the Transmission System Operation Rules of the TSO. Based on the plan, the TSO and DSOs are authorised to test the selected measures involved in the implementation of the Defence Plan and the Restoration Plan. With the entities which are involved in the Defence Plan and the Restoration Plan, the testing is limited only to specific measures, without implementing comprehensive testing/crisis scenario simulation.

The Emergency Plan was not approved at the national level as at the date of preparation of the Risk-preparedness Plan in the electricity sector. However, in accordance with the Test Plan and requirements of the restoration service providers, the tests of the selected measures aimed at preventing the interruption of the supply of electricity have been performed.

Agreements on emergency tests with the relevant neighbouring countries have not been signed to date. As a member of the international platform (see chapter 5.2 for details), Slovakia participates in the preparation of a memorandum of understanding that serves as the basis to intensify cooperation among Member States with respect to security of electricity supply and prevention and management of electricity emergencies with cross-border impacts. The preparation of an emergency testing schedule and procedures for its implementation will follow up on the signing of the MoU which will lay down the frameworks of cooperation among signatory Member States. The MoU is expected to be signed at the start of 2022.