economie
SPF Economie, P.M.E., Classes moyennes et Energie

Risk Preparedness Plan for the Electricity Sector

Content	The Risk Preparedness Plan contains both a national and regional risk assessment related to security of electricity supply. Building on the identified electricity crisis scenarios it identifies existing and planned measures to prevent, prepare for and manage electricity crises both on a national and regional level, in a spirit of solidarity and transparency and in full regard of the requirements of a competitive internal market for electricity. The risk Preparedness is established in line with the requirements pursuant to Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC.
Version	Draft 1
Latest version	16 March 2021
Competent Authority	Federal Minister of Energy
Contact	Be-riskpreparedness@economie.fgov.be
Region	Pentalateral Energy Forum (AT, BE, CH, DE, FR, LU, NL)

Content

Content 2

1. Summary of the electricity crisis scenarios 5

1.1 Regional electricity crisis scenarios 5

1.2. National electricity crisis scenarios 5

1.2.1 Cyberattack on business-critical infrastructure 8

1.2.2. Physical attack 8

1.2.2.1 Physical attack on critical assets 8

1.2.2.2. Physical attack on control centres 9

1.2.3. Insider attack 9

1.2.4. Storm 10

1.2.5. Winter incident ..... 11~~10~~

1.2.6. Cold spell 11

1.2.7. Heavy precipitation and flooding 11

1.2.8. Dry period and heatwave ..... 12~~11~~

1.2.9. Pandemic 12

1.2.10. Loss of ICT tools and public telecommunication ..... 13~~12~~

1.2.11. Accidental violation of N-1 criterion due to a human error 13

1.2.12. Fuel shortage ..... 14~~13~~

1.2.12.1. Fossil fuel shortage ..... 14~~13~~

1.2.12.2. Nuclear fuel shortage 14

2. Roles and responsibilities of the Competent Authority 15

3. Procedures and measures in the electricity crisis 16

3.1 National procedures and measures 16

3.1.1. Belgian implementation NIS Directive ..... 20~~19~~

3.1.2. Belgian implementation EPCIP Directive ..... 21~~20~~

3.1.3. The Law of 11 December 1998 ..... 22~~21~~

3.1.4. Belgian National Adaptation Plan 2017-2020 ..... 23~~22~~

3.1.5. Federal Network Development Plan ..... 25~~23~~

3.1.6 Resilience of the network infrastructure ..... 26~~25~~

3.1.6.1 Resilience of the network infrastructure against potential storms and vortexes: ... 26~~25~~

3.1.6.2 Resilience of the network infrastructure against heavy precipitation and flooding 27~~26~~

3.1.6.3 Resilience of the network infrastructure against water shortage ..... 27~~26~~

3.1.6.4. Resilience of the network infrastructure against technical faults ..... 28~~26~~

3.1.7. Permits ..... 28~~26~~

3.1.8. Test Plan ..... 28~~26~~

3.1.9 Operational Procedures ..... 31~~29~~

3.1.9.1 Procedure in case of an Electricity Shortfall ..... 32~~30~~

3.1.10.1.1 Detection and notification ..... 35~~33~~

3.1.10.1.2 Preparation of the crisis consultation (complete procedure) ..... 36~~34~~

3.1.10.1.3 Informing the crisis partners and the population (complete and shortened procedure) ..... 37~~35~~

3.1.10.1.4 Follow-up (complete and shortened procedure) ..... 37~~35~~

3.1.10.1.5 Load shedding (complete and shortened procedure) ..... 38~~35~~

3.1.10.1.6 Return to a normal situation (complete and shortened procedure) ..... 38~~36~~

3.1.9.2. Procedure in case of Sudden Phenomena ..... 38~~36~~

3.1.9.3. System Defence Plan ..... 39~~37~~

3.1.9.4 Load Shedding Plan ..... 40~~38~~

3.1.9.5 High Priority Significant Grid Users (HPSGUs) ..... 42~~39~~

3.1.9.6 Demand Reduction Measures ..... 42~~40~~

3.1.10. Business Continuity Plans ..... 43~~40~~

3.1.11. Restoration Plan ..... 43~~41~~

3.2. Communication mechanisms to inform the public ..... 45~~42~~

3.3. Market-based measures ..... 45~~43~~

3.4. Regional and bilateral procedures and measures ..... 46~~44~~

4. Crisis Coordinator..... 47~~45~~

5. Stakeholder consultations ..... 51~~48~~

5.1 Consultation of stakeholders ..... 51~~48~~

5.2 Consultation of the regional authorities..... 54~~50~~

5.3 Regional consultation ..... 54~~51~~

5.4 Further consultations..... 54~~51~~

6. Emergency tests..... 55~~52~~

6.1 Regional emergency tests ..... 55~~52~~

6.2 National emergency tests ..... 55~~52~~

Annex 1: Risk preparedness in the Pentalateral Energy Forum ..... 57~~54~~

1. Summary of the electricity crisis scenarios

1.1 Regional electricity crisis scenarios

The identification of the regional electricity crisis scenarios can be found in Annex 1. The regional electricity crisis scenarios were identified within a drafting team as part of the Pentalateral Energy Forum , Steering Group 2. The chapter in annex 1 also further describes the methodology applied for the identification of these regional electricity crisis scenarios, as well as the context of this Pentalateral Risk Preparedness Drafting Team.

1.2. National electricity crisis scenarios

In Accordance with article 7 of the Risk Preparedness Regulation (EU 2019/941), the Belgian Competent Authority, the Minister of Energy, identified 12 relevant national electricity crisis scenarios on 5 January, 2021, after consulting with the necessary stakeholders and considering the regional electricity crisis scenarios as defined in the ENTSO-E report of 7 September, 2020.

The identification of the national electricity crisis scenarios was based on a proposal discussed within the Risk Preparedness Stakeholder Task Force, which was established specifically for the purpose of the national implementation of the Risk Preparedness Regulation. The Task Force consists of the necessary stakeholders pursuant to article 7, section 2 of the Risk Preparedness Regulation, and is further described in chapter 5 that elaborates further on the stakeholder consultations.

Additionally, the regional authorities, meaning relevant representatives of the Flemish Region, the Walloon Region, and the Brussels-Capital Region, were consulted.

The proposal of the Risk Preparedness Stakeholder Task Force was based on a ranking of the different crisis scenarios discussed during the different stages of the process of identifying both the regional and the national crisis scenarios. A first selection of scenarios that was considered, was based on a national risk analysis performed by the National Crisis Centre (NCCN) in 2018. The 68 scenarios identified in the national risk analysis contained an overview of crisis scenarios that can give rise to national crises of which the impact is not limited to the energy sector. Within a working group consisting of the transmission system operator, the NCCN, and the Directorate-General for Energy, these scenarios were analysed based on their probability and possible impact on the security of electricity supply.

In accordance with article 7, section 3, of the Risk Preparedness Regulation, concerning the identification of national electricity crisis scenarios consistent with the regional electricity crisis scenarios, both the national assessment by the transmission system operator of the 31 regional electricity crisis scenarios as identified by ENTSO-E and a first ranking of the national assessment of the member states of the Pentalateral Energy Forum were taken into account. The schematic below gives an overview of the different steps and documents that were

considered for the identification of the national electricity crisis scenarios

Figure 1: Methodology for Identification

The scenarios identified by means of the documents and analyses mentioned above were then further assessed based on their relevancy for the security of electricity supply. In order to establish their relevancy, their national risk profile was taken into account. The methodology for allocating a national risk profile was based on the ENTSO-E Methodology, pursuant to article 5 of the Risk Preparedness Regulation. This means that every scenario was assessed based on its likelihood and on its possible impact on the security of electricity supply. *The likelihood as described for the different scenarios is in fact the likelihood the scenario will actually occur and will lead to an electricity crisis. For example, in case of the cold spell scenario, the likelihood is not limited to the likelihood the cold spell, with the different parameters as described, would occur, but it is the likelihood this cold spell would occur and would lead to an electricity crisis. To estimate this likelihood, the sum of the likelihood of the actual event with the estimation of the TSO of the likelihood this event would lead to an electricity crisis is made.* In order to be withheld in the final proposal of the national electricity crisis scenarios, the following conditions were taken into account:

- The scenarios that were identified as relevant, had a high impact - low probability risk profile;
- The scenarios in which the security of electricity supply was directly affected, and not affected as part of a spill-over effect, were withheld. This means for example that the scenario of a large industrial accident was not withheld, because the main consequences will not solely impact the security of electricity supply. At the same time, this also means that for example the scenario of the simultaneous failure of power system primary elements was not withheld since it is identified as a consequence of the already identified scenarios such as the various scenarios on extreme weather conditions.

After taking into consideration the methodology explained above, the Competent Authority decided on the 12 national electricity crisis scenarios as described in the table below.

SCENARIO GROUP	#	SCENARIO
Cyber Attack	1	Cyberattack on business-critical ICT infrastructure of entities which are physically connected to the power grid like TSOs, DSOs, power plants and major (industrial) loads.[1]
Physical Attack	2a	Physical Attack on Critical Assets
	2b	Physical Attack on Control Centres
Internal Attack	3	Insider Attack
Extreme Weather Conditions	4	Storm
	5	Winter Incident
	6	Cold Spell
	7	Heavy Precipitation & Flooding
	8	Dry Period & Heatwave
Natural Disaster(s)	9	Pandemic
Technical Failures	10	Loss of ICT tools and Public Telecommunication
	11	Accidental (unintended) Violation of N-1 Criterion due to a Human Error
Fuel Shortage	12a	Fossil Fuel Shortage
	12b	Nuclear Fuel Shortage

Table 1: National Electricity Crisis Scenarios

[1] To clarify this further, this concerns the business-critical ICT infrastructure of all entities connected to the power grid which would have a substantial impact in case an uncontrolled interaction with the power grid caused by a cyberattack on the business-critical ICT infrastructure would occur.

1.2.1 Cyberattack on business-critical infrastructure

Risk Profile	Impact	Likelihood	Cross-Border Impact
Major	Critical	Unlikely	Major

A cyberattack on business-critical infrastructure of entities, such as transmission system operators, distribution system operators, power plants and/or major industrial loads, which are physically connected to the power grid, would be aimed at the critical ICT systems of the targets mentioned above. Considered as part of this scenario are forms of hacktivism, serious cases of cybercrime, cyber threats from another state, cyberattacks initiated by a third party investor or cyberattacks from other private individuals or groups of people. Practically, this would mean that the person or the group of people performing the attack are able to manipulate the ICT systems from within. Furthermore, the attacker can also be able to complicate the process of restoration by blocking the users of the attacked systems.

Assuming that the attacker(s) targets several systems simultaneously, the scenario was given an overall major risk profile, taking into account its major risk for cross-border impact. Via a probabilistic calculation the likelihood of the scenario is assessed as being unlikely, but with a possible impact defined as critical. It is, however, important to note that both the national impact and the cross-border impact will strongly depend on the severity and duration of the attack. For the cross border consequences this means for example that when ICT systems of neighbouring TSOs are also affected, no mutual assistance is possible. Furthermore, if the cyberattack cannot be countered sufficiently fast, it might result in an electrical black-out.

1.2.2. Physical attack

The scenario related to a physical attack is divided into two sub scenarios based on the target of the attack, namely critical assets or control centres.

1.2.2.1 Physical attack on critical assets

Risk Profile	Impact	Likelihood	Cross-Border Impact
Major	Critical	Unlikely	Major

The scenario related to a physical attack on critical assets entails a violent attack on power lines, transformers, substations, powerplants and/or data centres. The violent attack can be carried out through various means ranging from a drone attack, hostage-taking, the use of explosives or other explosive devices, to an attempt at sabotaging physical infrastructure.

The scenario has an overall major risk profile with a major risk for cross-border impact. Through a probabilistic calculation the likelihood is assessed as being unlikely with the impact being assessed as critical. Specifically, this means that cross border energy exchange, reserve sharing and assistance can be severely compromised if cross-border network infrastructure components are damaged as well. In combination with unfavourable conditions such as adequacy issues, this could possibly lead to automatic load shedding. The impact depends on the amplitude, the severity, and whether attacks occur simultaneously. In the worst case scenario, when multiple critical network components are destroyed in parallel and repairing them will take up quite some time, the security of supply of a large amount of grid users could be severely compromised for a longer period of time.

1.2.2.2. Physical attack on control centres

Risk Profile	Impact	Likelihood	Cross-Border Impact
Major	Critical	Unlikely	Major

The scenario related to a physical attack on control centres entails a violent attack aimed at the control centres of the transmission system operators, the distribution system operators or of major power plants as well as their back-up facilities. The violent attack can be carried out through various means ranging from a drone-attack, hostage-taking, the use of explosive devices or an attempt at sabotaging the workings of the centres.

The scenario has an overall major risk profile with a major risk for cross-border impact. Through a probabilistic calculation the likelihood is assessed as being unlikely with the impact being assessed as critical. The impact, however, depends on the amplitude of the attack and whether several centres are targeted simultaneously. If, for example, multiple control centres are attacked at the same time, the remaining life of the grid will be of short duration. In case the attack only manages to target one centre, back-up control centres can take over control making sure the attack has a relatively small impact. Several back-up control centres and necessary evacuation procedures are in place. Furthermore, the main servers are situated in well-protected locations, meaning that when these locations are not targeted and they remain operational, the grid supervision can be performed from any location where secure IT connections remain possible.

1.2.3. Insider attack

Risk Profile	Impact	Likelihood	Cross-Border Impact
Major	Disastrous	Unlikely	Major

The scenario related to an insider attack entails deliberate sabotage carried out by an employee or a subcontractor, possibly initiated by a third party investor, a group, a state, or other private individuals. The attacker can either target the physical infrastructure, the virtual infrastructure or both. On top of the sabotage attempt, the attacker can also seek to blackmail key-employees or take these key-employees hostage during the attack.

The scenario has a major risk profile with a major risk for cross-border impact. Through a probabilistic calculation the occurrence of the scenario as a factor affecting the security of electricity supply is considered unlikely. At the same time, if the scenario occurs, a probabilistic calculation estimates that the impact would be disastrous. For example, if the attack leads to a grid collapse, cross-border energy exchange, reserve sharing and assistance might become impossible. If the insider opts for taking hostages instead of attacking the physical or virtual infrastructure, restoring the system could start as soon as the hostage-taking ends, without the need to repair the infrastructure.

1.2.4. Storm

Risk Profile	Impact	Likelihood	Cross-Border Impact
Major	Major	likely	Major

The initial conditions of this scenario involve a storm in large parts of Western Europe with expected wind speeds higher than 130 km/hour combined with wind gusts of over 150 km/hour. The consequences of these exceptionally strong wind gusts can severely affect electrical infrastructure components. Moreover, the flow of some interconnectors can be disturbed and even interrupted in case the specific network components are damaged due to the consequences of the storm.

The scenario has a major risk profile with a major risk for cross-border impact. Through an analysis of statistical data the occurrence of the scenario is assessed as likely, with a probabilistic estimation of having a major impact on the security of electricity supply. The stronger the wind speeds and wind gusts, the higher the risk that certain network elements will no longer be available. And although a storm usually has a rather local character, the impact on the network can be quite substantial.

Furthermore, the scenario can have an impact on offshore production in case production has to be shut down preventively. Especially with regards to the future this can increase the impact. For example, at the moment, large amounts of wind capacity are being installed in Dutch off-shore territory adjacent to the Belgian border, which will aggravate the loss of active power injected into the system.

At the same time, the scenario can also impact the national network. Over the last 100 years, the high-voltage grid in Belgium (70-380kV) has been build according to the applicable rules

of their construction year. The applicable rules have been amended over the past years, meaning that not all components are built with the same level of resistance. The most likely consequence and impact of a storm with wind speeds this exceptional will be the fragilization of the grid's integrity impacting end users.

1.2.5. Winter incident

Risk Profile	Impact	Likelihood	Cross-Border Impact
Major	Major	Possible	Major

The scenario related to a winter incident involves freezing and near-freezing temperatures around 0 degrees Celsius, in combination with high relative humidity and a peak in demand. This can cause wet snow to stick to overhead lines causing outages. In most cases this scenario will have a local character.

The scenario has a major risk profile with an estimation of major cross-border impact. Through statistical data the likelihood is assessed as possible with a probabilistic estimation of having a major impact on the security of electricity supply. Winter incidents such as described above can cause multiple outages that will fragilize the electrical network.

1.2.6. Cold spell

Risk Profile	Impact	Likelihood	Cross-Border Impact
Major	Major	Possible	Major

The scenario related to a cold spell involves a long period of extremely low temperatures of –20 degrees Celsius and lower, causing record levels of electric power consumption. Due to these record highs, unexpected outages of (thermal) power plants can occur. At the same time, multiple network components of the same type start failing unexpectedly during a relatively short period of time. This causes both adequacy issues due to the extreme high loads in combination with a lack of production capacity, and issues in transport capacity due to the failing network components.

The scenario has a risk profile of major and a major risk for cross-border impact. Based on statistical data, the scenario is assessed as having a likelihood of possible with a probabilistic estimation of having a major impact. Most likely the impact of the scenario will be load shedding by means of rolling black-outs.

1.2.7. Heavy precipitation and flooding

Risk Profile	Impact	Likelihood	Cross-Border Impact
Major	Major	Possible	Major

The scenario related to heavy precipitation and flooding involves continuous heavy rainfall in combination with spring tide, which in its turn causes flooding of significant parts of the country. The flooding of certain areas can cause unavailability of import generation, transmission and distribution infrastructure. This unavailability will fragilize the integrity of the grid creating an impact on end users.

The scenario has a risk profile of major with a major risk of cross-border impact. Statistical data proves the scenario to have a likelihood of possible with a probabilistic estimation of having a major impact. The impact will depend on the location of the floods, and on whether the impact remains local or on whether generation, transmission and distribution infrastructure is affected simultaneously on several locations.

1.2.8. Dry period and heatwave

Risk Profile	Impact	Likelihood	Cross-Border Impact
Major	Major	Likely	Major

The scenario related to a dry period in combination with a heat wave consists of a heatwave that lasts at least five days with average temperatures above 30 degrees Celsius and expected peak temperatures of 38 degrees Celsius and more. On top of this, this scenario is characterized by a longer period of little to no rainfall. The extremely high temperatures can cause multiple network components to unexpectedly start failing simultaneously in a relatively over a relatively short timeframe. Several additional network components or third party installations that support the grid, for example generators or compensators, continue to fail. These multiple failures of network components start affecting the available reserves, the flows to neighbouring countries and the supply to the end user. On top of this, the dry period causes several thermal power production units to lower production levels or to shut down completely due to insufficient means of cooling.

1.2.9. Pandemic

Risk Profile	Impact	Likelihood	Cross-Border Impact
Minor	Minor	Possible	Minor

The scenario consists of an internationally and even globally spreading virus. Although the current Covid-19 pandemic has not presented any severe consequences for the security of electricity supply, it cannot be excluded that a virus with a different profile would pose severe challenges. The risk mainly lies in personnel shortages and restrictions on movements of individuals, for example as part of containment measures, which can cause for example delays in maintenance.

Considering the different aspects, the scenario has an overall risk profile of minor, with a minor cross-border impact. It is estimated that mutual inter-TSO assistance will not be severely restricted. The likelihood based on statistics is considered possible, with a probabilistic estimation of the impact as minor.

1.2.10. Loss of ICT tools and public telecommunication

Risk Profile	Impact	Likelihood	Cross-Border Impact
Major	Critical	Unlikely	Major

This scenario involves the unavailability of a major part of the telecommunication infrastructure that is being used for operating the electricity market and/or the power system. It can also involve the unavailability of ICT systems that are crucial for real-time planning as well as operating the electricity market and/or the power system. The origin of the unavailability of the above mentioned systems is found in technical failures.

The scenario has an overall risk profile of major and an estimation of a major cross-border impact. The severity of the scenario strongly depends on the scale of the technical failures, the types of systems that are affected, whether systems are affected simultaneously and on the duration of the failures. In case, for example, the power system control cannot be restored sufficiently fast, the unavailability of these systems can cause an electrical black-out. If, on top of this, the ICT systems of neighbouring TSOs are affected as well, no mutual assistance will be possible. However, General Scada systems of different TSOs are, in most cases, established by different manufacturers. This reduces the risk for common mode failures.

Taking into consideration the conditions mentioned above, the impact of the scenario is probabilistically estimated as critical. According to statistical data, the scenario is unlikely to occur.

1.2.11. Accidental violation of N-1 criterion due to a human error

Risk Profile	Impact	Likelihood	Cross-Border Impact
Minor	Major	Unlikely	Major

Although the Belgian transmission system operator, Elia, has an internal quality system in place as well as strict safety rules, the scenario of a human error cannot be excluded. Even though strict safety rules are in place, a mistake made by the operators or the service staff can lead to cascading events. Cross border energy exchange, reserve sharing and/or mutual assistance might even become impossible in case the overhead lines between Belgium and the

Netherlands, Belgium and Luxembourg, Belgium and France, and/or network infrastructures close to the border are affected.

The scenario of a human error receives an overall minor risk profile, with the possibility of a major cross-border impact. Statistical data shows that the scenario is unlikely to occur, but if it does, a probabilistic calculation estimates this scenario would have a major impact.

1.2.12. Fuel shortage

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

1.2.12.1. Fossil fuel shortage

Risk Profile	Impact	Likelihood	Cross-Border Impact
Minor	critical	Very Unlikely	Major

The scenario of fossil fuel shortages involves a period with high national demand of fuel in combination with a low stock. The low stock can have several causes, in many cases connected to the above mentioned scenarios, such as weather conditions, a physical attack on infrastructure, or even political reasons. Although the scenario receives an overall minor risk profile, it is included to create a clear link between the crisis management policy for electricity supply as well as the other energy vectors in Belgium.

It is estimated that the scenario can have a major cross-border impact. For example, in case of fuel supply disruptions in Belgium, the transmission system operator, Elia, will not be able to provide inter-TSO assistance. If other countries are not affected in the same way by the fuel supply interruption, it would still be possible for their TSOs to provide assistance to Belgium.

According to statistical data the likelihood of the scenario is very unlikely, but in case it would occur a probabilistic calculation estimates the scenario to have a critical impact. In the evaluation of the scenario it was taken into account that Belgium has no endogenous fossil energy sources and therefore relies fully on fuel import. However, it is important to note that Belgium is strongly interconnected in order to allow import of several fuel types. This means that Belgium sources its fuel from different fuel suppliers across the world, and thus reduces the risk of disruption of supply.

1.2.12.2. Nuclear fuel shortage

Risk Profile	Impact	Likelihood	Cross-Border Impact
Minor	Major	Unlikely	Major

The scenario of a nuclear fuel shortage involves a low nuclear fuel stock in combination with high national electricity demand. The nuclear supply or production can in this case be

interrupted due to various reasons. As in the scenario of fossil fuel shortage described above, there are various reasons for the shortage to be found, varying from technical issues, malicious attacks, sabotage, political issues to extreme weather conditions.

Although Belgium is strongly dependent on nuclear power production, the overall risk profile was assessed as being minor, mainly due to the statistical unlikelihood. At the moment, Belgium has an installed capacity of 5,9 GW, but a progressive nuclear phase-out is planned to be finished by 2025. Taking into account the different aspects of the current situation, a probabilistic calculation estimates that a nuclear fuel shortage could have a major impact.

On top of this, it is also estimated that a nuclear fuel shortage in Belgium would have a major cross-border impact. In case of a nuclear fuel supply disruption in Belgium, Elia will no longer be able to provide inter-TSO assistance. For example, it also needs to be taken into account that when Belgium's neighbour France is affected by a nuclear fuel supply interruption, France will become a major importer, which will have a severe impact on the situation in Belgium.

2. Roles and responsibilities of the Competent Authority

Belgium has designated the Minister of Energy as Competent Authority pursuant to article 3 of the Risk Preparedness Regulation (EU) 2019/941. This designation was communicated in writing to the European Commission on 9 February 2020.

The Minister of Energy performs the roles and responsibilities of the Competent Authority since the nature and finality of the tasks attributed to the Competent Authority in the Risk Preparedness Regulation (EU) 2019/941 strongly align with the tasks that were attributed to the Minister of Energy in relation to electricity crisis management in the national legal and regulatory framework. In the notification letter to the European Commission it was, however,

also underscored that it might be preferable to make this designation explicit in national legislation. The objective is to have this achieved by the end of 2021.

Furthermore, in accordance with article 3, section 3 of the Risk Preparedness Regulation (EU) 2019/941, the following operational tasks regarding risk-preparedness planning and risk management have been informally and provisionally delegated to the Directorate General for Energy of the Federal Public Service for Economy, SME's, Self-Employed and Energy by the Competent Authority:

- Participate in the Electricity Coordination Group (ECG) and, where appropriate, prepare draft reactions to consultations launched within this forum pursuant to article 10, section 5;
- Preparing a proposal of national electricity crisis scenarios, to be approved by the Competent Authority pursuant to article 7, section 1;
- Preparing a proposal of assessment of the risks in relation to the ownership of infrastructure relevant for security of electricity supply, to be approved by the Competent Authority pursuant to article 7, section 4;
- Preparing a proposal for a draft and final Risk Preparedness Plan, to be approved by the Competent Authority pursuant to article 10, 11 and 12;
- Organize the necessary stakeholder engagement, public consultations and consultations of relevant European Union Member States and Third Countries pursuant to article 10, section 1, 4 and 5;
- Publish the final Risk Preparedness Plan on its website, while ensuring confidentiality of sensitive information pursuant to article 10, section 7.

The delegated tasks as described above, are performed under the supervision of the Competent Authority.

3. Procedures and measures in the electricity crisis

3.1 National procedures and measures

The national electricity crisis scenarios as identified in chapter 1.2 of this Risk Preparedness Plan, serve as the basis for the identification of the existing and planned measures and procedures to prevent, prepare for and mitigate the consequences of a possible electricity crisis. The table below serves to provide an overview of the identified national electricity crisis scenarios and the different identified national plans, measures and procedures. The overview table will help to identify potential gaps by analysing whether the risks related to the identified electricity crisis scenarios are sufficiently covered by the identified measures.

During the process of identifying the existing and planned national measures, three definitions of types of measures were established, pursuant to what is required in the Regulation (EU) 2019/941. The three different types of measures identified, are the following:

- **Preventive measures**: Measures that are in place, or that are planned, to prevent the occurrence of the identified electricity crisis scenarios;

- **Preparedness measures**: Measures that are in place, or that are planned, to prepare a response to an imminent crisis (e.g. preparedness measures taken as part of the procedure in case of electricity shortfall) ;

- **Emergency Response measures**: Measures that are in place, or that are planned, to mitigate the consequences of an electricity crisis.

Nevertheless, it is important to note that not all identified measures fit into one of these clear-cut definitions. For example, the procedures in case of an electricity shortfall cannot easily be defined as one of the three types of measures described above. The procedure contains the possibility of activating different types of measures depending on the point in time and the severity of the crisis.

The following chapters will briefly describe the measures as identified in the table below, and will indicate in what way they respond to the identified national electricity crisis scenarios.

		Measures							
		NIS	EPCIP	Law of 11 December 1998 (Security Clearances)	National Adaptation Plan	Federal Network Development Plan	Permits	Test plan	Shortfall Procedure
Risk Scenarios	Cyber Attack	X		x					X
	Physical Attack		x	X (attack against control centres)					X
	Inside Attack	x	x	X					X
	Storm				X	x	x		X
	Winter Incident				X	x	x		X
	Cold Spell				X	x	x		X
	Flooding				X	x	x		X
	Dry Period & Heatwave				x	x	x		X
	Pandemic								x
	Loss of ICT/public telecom							X	X
	Human Error			x					X
	Fuel shortage								x

Table 2: Preventive and Preparedness Measures

		Procedure Sudden Phenomena	System Defence Plan	BCP	Restoration Plan
Risk Scenarios	Cyber Attack	X	X	X	X
	Physical Attack	X	X		X
	Inside Attack	X	X		X
	Storm	X	X		X
	Winter Incident	X	X		X
	Cold Spell	X	X		X
	Flooding	X	X		X
	Dry Period & Heatwave	X	X		X
	Pandemic	X	X	X	X
	Loss of ICT/public telecom	X	X	X	X
	Human Error	X	X		X
	Fuel Shortage	X	X		x

Table 3: Preparedness and Emergency Response Measures

3.1.1. Belgian implementation NIS Directive

The European Network and Information System Security Directive (NIS), Directive 2016/1148 of July 6, 2016 on measures to ensure a common high level of network and information system security in the Union, has been implemented in Belgian legislation by the Law of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security, as mentioned in the first chapter.

The Minister of Energy has been designated as the sectoral authority for the energy sector. The administration of the sectoral authority has taken into consideration the different stakeholders of the electrical energy sub-sector (producers, distributors, suppliers, traders, data analysts, ...). For the identification as it is today, the sector authority applies the following criteria:

- The entity provides a service that is essential for the maintenance of critical societal and/or economic activities;
- The provision of essential services depends on information networks and services;
- An incident would be likely to have a significant disruptive effect on the provision of such service.

In order to determine the significance of the disruptive effect, the sectoral authority considers sectoral and/or cross-sectoral criteria and decides on the thresholds and levels deemed appropriate:

- The number of dependent users;
- Dependence of other sectors on the service;
- The consequences of incidents in terms of duration and degree on societal, economic or public safety functions;
- The entity's market share;
- The size of the geographical area likely to be affected in the event of an incident;
- Consideration of alternatives for the provision of this service.

Operators meeting these criteria are identified as essential service operators. By default, and in the absence of evidence to the contrary, the operation of a critical infrastructure identified under the EPCIP Law, is presumed to be dependent on information systems The operator of a critical infrastructure is therefore automatically identified as an operator of essential services under the NIS Law.

The operator of essential services notified as such by the sector authority develops the necessary technical and organizational measures to manage security threats to networks and information

systems. These measures constitute the Information Systems Security Policy (ISP) and must meet the requirements of ISO/IEC 27001 Information Security Management Systems standard or an equivalent, subject to audit and inspection. In the operator's ISP, measures to prevent and/or mitigate potential cyber and insider attacks are implemented. The ISP measures implemented by both the operator and potential digital service providers are inspected and audited on a regular basis.

By ensuring the implementation of the ISP measures, the Belgian NIS legislation is identified as being able to mitigate the risks connected to the possible occurrence and consequences of a cyber attack and/or an insider attack.

3.1.2. Belgian implementation EPCIP Directive

The European Directive 2008/114/EC of December 8, 2008 on the identficiation and designation of European Critical Infrastructures and the assessment of the need to improve their protection, als referred to as "EPCIP" (European Program for Critical Infrastructure Protection) has been implemented in Belgian legislation through the Law of July 1, 2011 on the security and protection of critical infrastructure (EPCIP Law). Applied to the electric power sector, it aims to raise the level of protection of electricity generation and transmission infrastructures, apart from nuclear facilities.

The National Crisis Centre (NCCN) is the point of contact in Belgium for the EPCIP Law. The sectoral authority, the Minister of Energy and, by delegation, her administration, carry out the evaluation and identification of critical infrastructures, based on sectoral criteria, in consultation with the NCCN. These criteria are :

- The potential impact in terms of the number of victims or injured;
- The potential economic impact including the extent of economic loss and/or degradation of products or services, including environmental impact;
- The potential impact on the general public, including on public confidence, physical suffering and disruption of daily life, including the loss of essential services.

These levels are based on the severity of the impact of the disruption or destruction of a given infrastructure. At the end of this identification process, a list of critical infrastructures in Belgium was established during the first implementation cycle of the law, that is during the period between 2015 and 2019. The law imposes a periodic re-valuation of critical infrastructures.

The operator of the critical infrastructures is notified of the decision and is required to implement internal and external security measures for the identified infrastructure. In practice, within one year after receiving the notification, the operator must establish an Operator Security Plan (OSP) for every identified site. This OSP includes at least :

- The location and inventory of the various points of the infrastructure which, if they were affected, could cause the interruption of its operation;
- A risk analysis consisting of the identification of different relevant potential threat scenarios of intentional acts aimed at destroying or interrupting the operation of the critical infrastructure. These scenarios include the various possibilities of physical attacks and insider attacks against the infrastructure;
- An analysis of the vulnerabilities of the various points of the infrastructure and their potential impact of disruption or destruction according to the different scenarios identified;
- For each scenario of the risk analysis, the identification, selection and prioritization of internal security measures.

The critical infrastructures are subject to inspections by the sectoral authority in order to verify the proper implementation of these measures. The operator is required to organize regular exercises in relation to these scenarios.

The NCCN is responsible for external protection measures, based on a threat analysis provided by the Coordinating Body for Threat Analysis.

The measures and inspections mentioned above in light of the Belgian EPCIP Legislation are identified as measures to mitigate the risks connected to the national electricity crisis scenario of a physical attack. By implementing these measures that mitigate the risk of a physical attack, the possibility of a successful insider attack also diminishes.

3.1.3. The Law of 11 December 1998

The Law of December 11, 1998 on "classification, security clearances, security certificates and security advises", provides a legal basis to regulate the classification of items and the access to these classified items. The items that can be classified are, among others, information, documents, data or material, of which inappropriate use could harm national interests, such as the national security and the national scientific and economic potential.

Next to the classification and access to classified items, the Law also provides a legal basis for the so-called 'security advises'. The security advises give vital companies the opportunity to have their

personnel screened by the public authorities, who, due to the nature of their profession, function, mission or mandate or due to their access to specific sites, or due to the possession of a certain license or allowance, could harm national interests. In order to determine which employees should be subject to such screening, the company concerned should make a risk analysis and motivate thoroughly why inappropriate use of the company assets could pose a risk for the national interests. This mechanism is also applicable in the electricity sector. The sectoral authority that is responsible for the application of the "security advises" in the energy sector, is the Minister of Energy.

The screening of personnel as part of the Law of December 11, 1998 is identified as a measure to prevent and/or mitigate the risks of a possible insider attack as identified in chapter 1.2.

3.1.4. Belgian National Adaptation Plan 2017-2020

The Belgian National Adaptation Plan for 2017-2020 proposed a set of national measures that focused on adaptation to climate change and its consequences. The plan contains several measures that help mitigate the risks related to the national electricity crisis scenarios regarding extreme weather conditions as identified in chapter 1.2. The Belgian National Adaptation Plan realistically focusses on adaptation measures since even the most severe mitigation efforts will not be able to help avoid consequences caused by current and future climate change. Adaptation measures are therefore necessary to reduce the unavoidable impact linked to climate change. The complete Belgian National Adaptation Plan 2017-2020, can be consulted on the Belgian federal site dedicated to information on climate change.

Field Code Changed

Three different measures identified in the Belgian National Adaptation Plan are relevant in the context of the Risk Preparedness Plan and the electricity crisis scenarios identified in chapter 1.2.

- Measure 1: Development of high resolution climate scenarios for Belgium;
- Measure 6: Evaluate the impact of climate change on the security of the energy supply and the energy transport and distribution infrastructures;
- Measure 10: Promote transnational cooperation on adaptation

Measure 1, the development of high resolution climate scenarios for Belgium, is a first useful step in mitigating the risks connected to the scenarios related to extreme weather scenarios. The goal of this measure was to establish new climate scenarios to be used as national reference for future impact and vulnerability assessments by 2017. In order to best anticipate the future consequences

of climate change, high resolution scenarios that are adapted to the needs of different sectors, e.g. the energy sector, are needed. In 2013, a federal scenario platform was created to bring together the most important scientific players to exchange the necessary information in order to create coherent scenarios. This federal platform and the creation of national scenarios is also important to create scenarios that stimulate a coherent national approach to the consequences of climate change. It also allows to identify the most relevant consequences of climate change for Belgium, such as the crisis scenarios identified in chapter 1.2, for example heatwaves, drought, and floods.

In this context, CORDEX.be[2], presented its results in 2017. These presented scenarios will serve as reference cases. Several new climate projections were developed for Belgium as part of the CORDEX.be project. This project grouped all the Belgian research activities related to climate modeling. Strict agreements were made within this group regarding the coherence of climate projections. Therefore, the model projections in all respects follow the international conventions as drawn up in the latest report of the IPCC (for global projections), the one prepared by CORDEX (for regional projections) as well as new conventions for the Belgian climate groups. The positioning of the Belgian results within an international context makes it possible to estimate the impact of climate change and the associated uncertainties, which makes it possible to predict associated risks. A large database of climate projections has been compiled, of which the spatial and temporal detail is greater than that prescribed by international initiatives. This database allows to study the impact of climate change for different sectors. On the one hand, several exploratory impact studies have already been carried out with regard to agriculture, heat waves, extreme rainfall, the urban heat island, biogenic emissions (important for healthcare) and storms. On the other hand, the short duration of the initial project did not allow for in-depth analyses to be carried out based on all of the data and phenomena. Such studies, however, are needed as a solid basis for adaptation decision-making.

The goal of measure 6 is to evaluate the impact of climate change on the security of the energy supply and the energy transport and distribution infrastructures. This evaluation will help develop the necessary knowledge about climate change consequences on the energy sector by raising the awareness of the possible threats it causes. The study will be a collaboration between regional and federal governments in order to improve and better coordinate energy knowledge. The final goal of this evaluative study will be to specify recommendations that will improve the energy sector's resilience when it comes to facing the consequences of climate change.

[2] http://cordex.meteo.be/meteo/view/en/19292661-+Cordex.be.html

Measure 10 aims to promote transnational cooperation on adaptation to the consequences of climate change in order to increase the transnational coherence of the adaptation policies, especially among neighboring countries that often share common interests, but also common issues. Additionally, it provides a framework for possibilities to learn more easily from one another and to exchange information on best practices. In light of this measure, the focus was specifically put on the possibility of creating a Benelux partnership with an important focus on the cross-border risks for the energy sector. During the period between 2017 and 2020 several exercises and workshops took place in order to establish this. Within the Benelux structure Belgium will continue to participate in the organization of different workshops.

The measures mentioned above not only help to raise awareness to the need for adaptation policies, they also help to identify specific consequences of climate change on the energy sector in more detail. By putting efforts in studies of identifying both national and transnational impacts, it lays down the basis for further improvements of the sector's resilience to the impact of climate change, and in this case, more specifically, the consequences of scenarios related to extreme weather conditions.

3.1.5. Federal Network Development Plan

The Federal Network Development Plan has a positive preventive impact on the risks identified in chapter 1.2. A more developed grid foresees the required adequacy and security for withstanding disruptive events as described in the national crisis scenarios. This is done by a reinforcement of the interconnections with neighbouring countries and by reinforcing the national grid. Removing internal bottlenecks through reinforcements of certain corridors also has a positive impact on the interconnection capacity with neighbouring countries.

The Federal Transmission Grid Development Plan 2020-2030 contains a full description of the planned projects to increase the interconnection capacity. The main focus of the planned investments related to import is the enhancement of the internal grid in order to handle all the possible import capacity and increase the redundancy of the grid. By 2035, almost the entire 380 kV backbone will be upgraded to HTLS (High Temperature Low Sag technology), allowing for further cross border reinforcements. To accommodate for the future increase in offshore wind production, combined with higher imports from the UK and France, two new internal corridors are planned. One corridor, called "Ventilus", foresees in an enhancement of the capacity from the Belgian shore in order to handle the increased offshore wind injection and a second HVDC interconnector. A second corridor, named "Boucle du Hainaut", will increase the capacity in order to transport more electrical power from west to east and therefore increasing the ability to handle and transport further import from France and the UK, in combination with a high offshore wind production.

Besides the multiple enhancements on the internal grid, the cross-border interconnectors will be upgraded as well. On the Northern border with The Netherlands, an upgrade of the grid is foreseen by reinforcing the line configuration and installing Phase Shifting Transformers to optimize the flows in that region. Further plans to optimize the grid situation in that region are under investigation .

On the Southern border with France, there are three interconnection corridors. The most Northern corridor "Avelgem-Avelin" will undergo the installation of HTLS lines to increase its capacity. Phase Shifting Transformers will be installed on the corridor "Achène-Lonny" to optimize the current flows. On both borders additional plans are being analyzed in order to further optimize the grid for a stable import capacity. A second interconnector with the UK, a second interconnector with Germany, and a first interconnector with Denmark are being investigated as well. The Federal grid development plan 2024 – 2034 will elaborate more on these future plans and projects.

The conclusion to be made is twofold.. On the one hand, Elia will increase its simultaneous import capacity to 7500MW once MVAR investments are realized. On the other hand, Elia is reinforcing the internal grid to be able to handle all possible import capacity. By 2035, almost the entire 380 kV backbone will be upgraded to HTLS, allowing for further cross border reinforcements.

Every four years Elia establishes this Federal Grid Development Plan to assess whether further investments and developments are needed in order to improve the condition of the grid. Elia publishes the latest version of this plan on its website.

3.1.6 Resilience of the network infrastructure

Improving the resilience of the network infrastructure is an important preventive measure, mitigating the risks connected to several of the electricity crisis scenarios identified in chapter 1.2.

3.1.6.1 Resilience of the network infrastructure against potential storms and vortexes:

Over the past 100 years, Belgium's 70-380 kV high-voltage grid has been built in accordance with the rules applicable in the relevant year of construction. We distinguish between the construction classes in terms of reliability, with the reference wind at a height of 50m being provided in each case, in the table below.

The 380kV network is built for >70% in accordance with the 1958 Royal Degree "1qb", the rest in accordance with AREI/RGIE "2qb". The other voltage levels are more spread out.
The reference wind speed increases over time. New pylons from 150kV onwards are constructed with the highest reliability, with respect to wind, given their greater impact on security of supply.

Time to repair in case of damage depends on the storm's intensity. Setting up an emergency overhead line takes up a minimum of two weeks.

From year [3]	Construction reliability-class (CRC)		Wind at extreme loading [km/h] at 50m height
1920	Royal Degree		175
1931	Royal Degree + broken cable		172
1958	Royal Degree basic windpressure "1qb"		**149**
1985	AREI/RGIE windpressure "2qb"		**184**
2020	Design overhead line cfr. EN50341 – windspeeds: see EN1991 Tabel 4.9 ANB: Extreme windpressure $q_p(z)$ (N/m²) $v_{b,0}$: 26 m/s en c_o =1 surface category II	Reliability Level 1 – 70kV concrete poles	174
		Reliability Level 2 (New 70-110kV metallic & concrete towers)	**191**
		Reliability Level 3 (New 150, 220, 380kV towers)	**206**

Table 4: Construction reliability-class

3.1.6.2 Resilience of the network infrastructure against heavy precipitation and flooding

The north of Belgium is located close to the estuaries of the rivers Schelde and Maas. Key substations are in the immediate vicinity of those rivers. In case of extreme floods, which has a very low probability, these substations are affected and have a major impact.
Control centers and data centers of the transmission system operator are in low-risk zones when it comes to flooding.

3.1.6.3 Resilience of the network infrastructure against water shortage

Dry periods and low water levels across large parts of Europe cause lack of production in several countries. Most large power producing facilities in Belgium are located near large rivers with moderate risks for power production capability reduction because of insufficient cooling means. In extreme events, no mutual assistance across borders might be possible.

[3] The given year represents the year when the directives were officially applied. This does not necessarily mean that the construction put into service that year is in line with the directives, this can only be verified through the calculation notes.

A lack of generation capacity together with a lack of import capabilities could lead to a scarcity situation. In such cases, restrictions in use of electricity for certain targets or rolling blackouts will be applied.

3.1.6.4. Resilience of the network infrastructure against technical faults

The risk for unexpected outages of a series of infrastructure components of the same type is minimized by applying preventive asset management and continuous improvements. The TSO's certified internal quality system and indoctrinated safety rules should reduce the likelihood of human errors. Resilience against simultaneous failure of power system primary elements depends on the number of simultaneously affected infrastructure elements. The likelihood of spontaneous outages of multiple elements in independent substations is very unlikely, however, the impact of this might be critical.

3.1.7. Permits

Chapter will be completed by the DG Energy-FPS Economy before the deadline for the draft proposal

3.1.8. Test Plan

The Test Plan is elaborated by Elia, taking into account the prescriptions of Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration (NC ER) and taking into account other relevant legislation (e.g. the Federal Grid Code) and other Network Codes RfG, DCC and HVDC. The Test Plan describes the tests, the frequency of the tests, and the conditions for the tests that are applied to defence and restoration service providers and identifies the equipment and capabilities relevant for the System Defence Plan and the Restoration Plan that have to be tested. A short description of both the System Defence Plan and the Restoration Plan can be found in the chapters below.

The following table specifies the identified equipment and capabilities relevant for the System Defence Plan and the Restoration Plan that have to be tested, pursuant article 43, section 2 of the Regulation (EU) 2017/2196.

/Equipment and capabilities relevant for the System Defence Plan and/or Restoration Plan that have to be tested	Relevant for System Defence Plan or Restoration Plan or general obligation	Periodicity of the tests	Remarks
RSP which is a PGM delivering a black start service	Restoration Plan	3 years	Conditions of the tests are included in paragraph 4.1

The SGUs identified pursuant to point (c) of Article 11(4) of NC ER that do not ressort under the NC RfG, NC HVDC or NC DCC (existing installations)	System Defence Plan	Once during the connection process	For facilities that need to activate defence or restoration measures at the request of ELIA without a contractual basis, the capacities are tested during the connection process. ELIA will not impose any defence or restoration measures which exceed the capacity of the installation(s) specified in the connection contract, as stated in paragraph 8.
The SGUs identified pursuant to point (c) of Article 23(4) of NC ER that do not ressort under the NC RfG, NC HVDC or NC DCC (existing installations)	Restoration Plan		
The SGUs identified pursuant to point (c) of Article 11(4) of NC ER that ressort under the NC RfG, NC HVDC or NC DCC new installations)	System Defence Plan	Once during the connection process	For facilities that need to activate defence or restoration measures at ELIA's request without a contractual basis, the capabilities were tested during the connection process as described in the NC RfG, NC HVDC or NC DCC. ELIA will not impose defence or restoration measures which exceed the capacity of the installation(s) specified in the connection contract, as stated in paragraph 8.
The SGUs identified pursuant to point (c) of Article 23(4) of NC ER that ressort under the NC RfG, NC HVDC or NC DCC new installations)	Restoration Plan		
LFDD relays implemented on TSO, public DSO of CDSO installations (if any)	System Defence Plan	10 years	Conditions of the tests are included in paragraph 7
Communication systems defined in art 41 of the NC ER of ELIA, RSPs, public DSOs, CDSOs and SGUs identified in the Restoration Plan	General obligation according to NCER art 48(1)	1 year	Conditions of the tests are included in paragraph 9.1
Backup power supply of communication systems of ELIA, RSPs, public DSOs, CDSOs and SGUs identified in the Restoration Plan	General obligation according to NCER art 48(2)	5 years	Conditions of the tests are included in paragraph 9.2
Inter-TSO communication systems	General obligation according to NCER art 48(3)	Periodicity to be defined by 18/12/2024	Conditions of the test to be defined by 18 December 2024
Communication systems between ELIA and Coreso	General obligation according to NCER art 49(2)	3 years	Conditions of the tests are included in paragraph 9.1
Notification system for Emergency ELIA, Black-out ELIA, Grid Restoration ELIA	System defence plan and restoration plan	1 year	Conditions of the tests are included in paragraph 9.3

Main and backup power sources to supply ELIA's main and backup control rooms, provided for in art 42 of the NC ER	General obligation according to NCER art 49(2)	1 year	Conditions of the tests are included in paragraph 10.1
ELIA's backup power sources to supply essential services of the substations identified as essential for the Restoration Plan procedures	General obligation according to NCER art 49(2)	3 years	Conditions of the tests are included in paragraph 9.1
			(*)
ELIA's backup power sources to supply essential services of the substations identified as essential for the Restoration Plan procedures	General obligation according to NCER art 49(3)	5 years	Conditions of the tests are included in paragraph 10.2
			(*)
ELIA's transfer procedure for moving from the main control room to the backup control room	General obligation according to NCER art 49(4)	1 year	Conditions of the tests are included in paragraph 10.3
Signal for reducing voltages in distribution networks by 5% (U-5%)	System Defence Plan	5 years	The conditions of the tests are included in paragraph 11.
Synchronous coupling devices	Restoration Plan	During daily operations	The conditions of the tests are included in paragraph 12.
Limited frequency sensitive mode for under frequency and over frequency of power generation modules of type C and D	System Defence Plan	At least after 10 years or after significant modifications	The conditions of the tests are included in paragraph 4.2.
Limited frequency sensitive mode for under frequency and over frequency of HVDC-installations that interconnect different synchronous areas.	System Defence Plan	At least after 10 years or after significant modifications	The conditions of the tests are included in paragraph 6.1.
(*) In case public DSOs, CDSO of SGUs are involved in these tools and facilities, they participate to this test.			

Table 5: Test Plan

The most recent version of the Test Plan can be consulted on the website of Elia.

Field Code Changed

As this version of the Risk Preparedness Plan was drafted, the Test Plan was waiting for approval by the Minister of Energy.

3.1.9 Operational Procedures

In case the different preventive measures described in the chapters mentioned above are not sufficient to mitigate the risks connected to the electricity crisis scenarios as identified in chapter 1.2, several operational procedures, plans and measures are in place to prepare for the consequences of a possible crisis and to mitigate these consequences. The chapters below describe these different procedures in more detail. In order to fully grasp the background of these procedures it is useful to have an overview of the national legislative background of electricity crisis management in Belgium.

At the moment, the national legal framework for electricity crisis management consists of two key documents:

- The Royal Decree of 22 April 2019 on the technical regulation concerning the operation and access to the transmission network (The Federal Grid Code);
- The Ministerial Decree of 3 June 2005 on the establishment of the load-shedding plan of the electricity network.

The Federal Grid Code of 22 April 2019, specifically article 261 §4, creates a legal basis for the Ministerial Decree of 3 June 2005 on the establishment of the load-shedding plan of the electricity network. In turn, the load-shedding plan as defined in this Ministerial Decree, is embedded in the System Defence Plan, which finds it origin in articles 11 to 22 of the Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration (NC ER).

The transmission system operator, Elia, has developed a global load-shedding plan that can either be activated automatically in the event of an incident on the high-voltage network or that can be activated manually in the event of an electricity shortfall. The measures to restore an imbalance on the electrical system vary considerably depending on the cause of the supply disruption: either a sudden phenomenon or a predicted electricity shortfall. This decree therefore includes the following procedures:

- The procedure for protection against sudden phenomena;
- The procedure for protection against a predicted electricity shortfall.

During the ongoing implementation of the Risk Preparedness Regulation, a review of the Ministerial Decree of 3 June 2005 on the establishment of the load-shedding plan of the electricity network, as well as the Federal Grid Code, taking into account the requirements of the Risk Preparedness Plan, is scheduled.

The schematic below provides an overview of the different measures, that will be described in more detail in the following chapters.

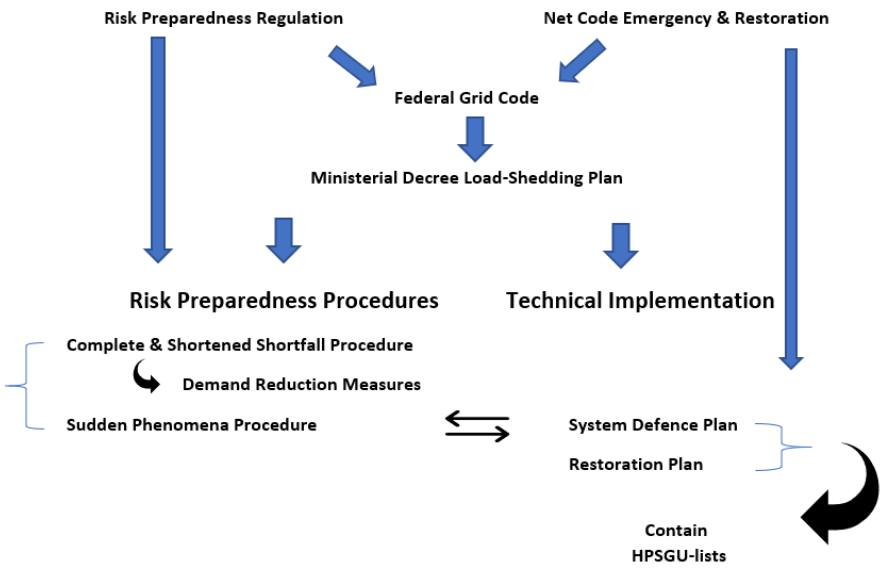

Figure 2: Operational Procedures

3.1.9.1 Procedure in case of an Electricity Shortfall

In order to manage a predicted electricity shortfall, a common procedure has been developed by the Directorate-General for Energy of the Federal Public Service (FPS) of Economy, SMEs, Self-Employed and Energy and the National Crisis Center (NCCN) of the Federal Public Service (FPS) of the Interior, in close cooperation with the transmission network operator, Elia, and the Federation of Electricity and Gas Operators in Belgium, Synergrid. The procedure in the event of an electricity shortfall (hereinafter referred to as "the shortfall procedure") aims to coordinate the actions of the partners mentioned above on the following aspects:

- Notification of a threat of a shortfall and notification of an actual shortfall;

- Taking actions to maintain and/or restore the balance of the adjustment zone or reduce local energy shortages and;
- Preparation for the management of a possible activation of the load shedding plan in the event of a shortfall and the consequences of this activation.

This procedure is based on the principles of relevant national legislation, the structure of the federal crisis management, the involvement of various actors of the crisis cells and the information on which Elia can take the decision and notify the government partners if a threat of a shortfall or an actual shortfall occurs. Based on the moment on which Elia detects and notifies a threat of a shortfall, either the shortened or the complete shortfall procedure is applied. A threat of a shortfall can be detected and announced by Elia at the earliest seven days (Day D-7) before the day of the actual shortfall (Day D). In case Elia has detected and notified a threat of a shortfall between Day D-7 and Day D-2 before 7 pm, the complete shortfall procedure will be applied. The schematic below visualizes the scope of the complete shortfall procedure.

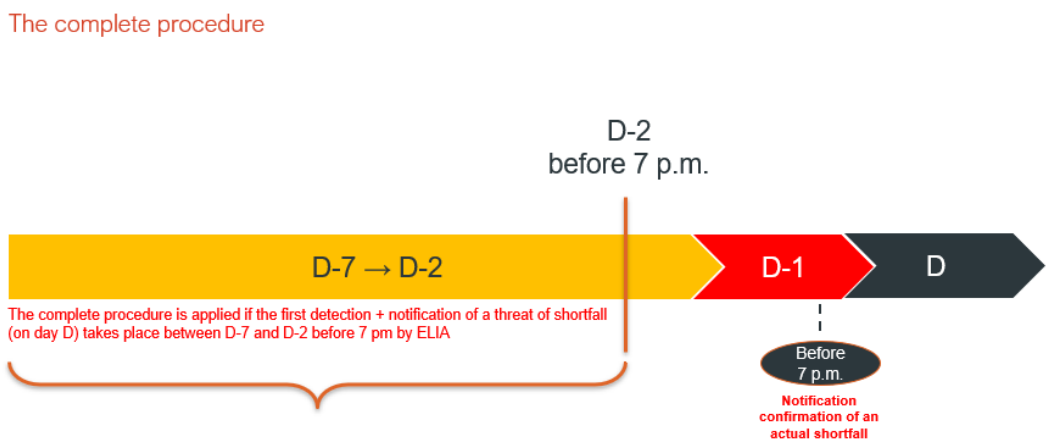

Figure 3: Complete Shortfall Procedure

However, in case Elia has detected and notified a threat of a shortfall between Day D-2 after 7 pm and Day D-1 before 7 pm, the shortened procedure will be activated, since there is not enough

time left to go through the complete procedure. The schematic below visualizes the scope of the shortened shortfall procedure.

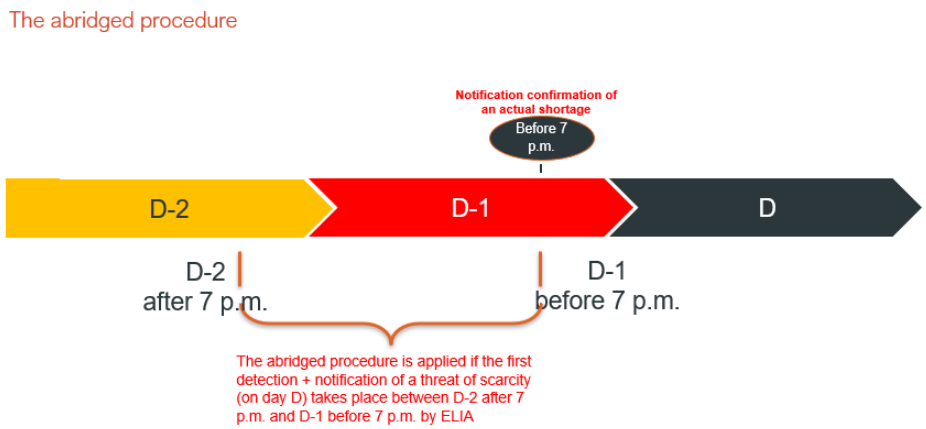

Figure 4: Shortened Shortfall Procedure

The shortfall procedure consists of the following four chapters:

1. The first chapter comprises the complete procedure and entails the following phases:
    a. Detection;
    b. Notification;
    c. Preparation for crisis consultation;
    d. Crisis consultation;
    e. Communication about the decisions taken;
    f. Coordination of measures and informing the population;
    g. Follow-up and;
    h. Return to a normal situation or transition to an actual electricity shortfall.

2. The second chapter describes the phases of an actual shortfall, following a detection and a notification of a threat of a shortfall in the preceding day(s):
    a. Confirmation of an actual shortfall;
    b. Notification;
    c. Crisis consultation / management cell;
    d. Communication about the decisions taken;
    e. Coordination of the measures and informing the population;
    f. Follow-up and;
    g. Return to a normal state.
3. The third chapter includes the phases of the shortened procedure:
    a. Detection;
    b. Notification;
    c. Organization of the first moments of crisis management;
    d. Crisis consultation / management cell;
    e. Communication about the decisions taken;
    f. Coordination of the measures and informing the population;
    g. Follow-up and;
    h. Return to a normal state or the transition to an actual electricity shortfall.
4. Chapter 4 describes the return to a normal state after a threat of a shortfall or after an actual shortfall.

3.1.10.1.1 Detection and notification

Elia can detect a threat of a shortfall by analyzing:

- the forecasts of the Royal Meteorological Institute (RMI);
- the production prospects and;

- the information from the energy markets.

As soon as a threat of a shortfall is detected, Elia informs the following government partners:

- the Federal Ministers of Energy, of Economy, of Mobility and of Public Health;
- the Minister of the Interior;
- the Regional Ministers of Energy and;
- the Directors-General of the Directorate-General for Energy and the Directorate-General for the National Crisis Center.

In case the complete shortfall procedure is applied, Elia invites the partners mentioned above to a technical briefing, which takes place as soon as possible after the notification by Elia. Elia explains he threat of a shortfall in more detail based upon:

- its cause;
- the moment of the shortfall;
- the estimated impact of the shortage;
- the expected duration;
- the size of the shortage and;
- the day on which the actual shortfall is to be expected.

Elia also proposes a set of measures to avoid or to limit the expected electricity shortfall.

In case the shortened procedure is applied, there is no time for a technical briefing and for preparing the crisis consultation. In this case the NCCN invites all members of the crisis cell in order to organize the first moments of the crisis consultation.

3.1.10.1.2 Preparation of the crisis consultation (complete procedure)

A first step is taken by the FPS Economy by convening the members of the departmental crisis cell of their departmental crisis cell. One of the tasks of this crisis cell is to analyze the package of measures that may be eligible to limit the demand for electricity. These will differ depending on the order of magnitude of the expected electricity shortfall and on the feasibility of the measures. Subsequently the members of the information cell prepare a communication strategy.

If the situation allows it, the relevant members of the Federal Coordination Committee will meet prior to the crisis consultation. This decision will be made at the end of Elia's technical briefing.

The members will analyze the consequences of the situation on the individual and collective security and propose measures.

During the crisis consultation and after consulting with the members of the management cell, the Federal ministers of Energy and of Economy will decide which measures can be taken to limit the possibility of the predicted electricity shortfall. If necessary, the Minister of the Interior also participates in these crisis consultations in order to take measures to ensure public order and individual and collective security.

3.1.10.1.3 Informing the crisis partners and the population (complete and shortened procedure)

During the crisis consultation it is also decided when and how the population will be made aware of the threat of a shortfall and the measures planned. The Federal Ministers of Energy and of Economy can consult with the members of the information cell on this topic.

The NCCN distributes the information to the following crisis partners:

- the Ministers-President of the regions;
- the mayors (via the governors of the provinces);
- the "disciplines"[4] 1 to 4, containing:
    - the emergency call centers100 and 112;
    - the FPS Public Health;
    - the Directorate of the Operations of Administrative police (DAO) of the Federal Police;
    - Civil Protection and the Ministry of Defense,
- other ministers and their departmental crisis cells and;
- the Belgian Institute for Postal Services and Telecommunications (BIPT).

3.1.10.1.4 Follow-up (complete and shortened procedure)

[4] Every emergency situation will be mitigated by teams of people. In Emergency Planning there are five different Disciplines that coordinately work during an emergency situation. Discipline one consists of the emergency relief operations such as fire fighters, Civil Protection and specialists. Discipline two consists of medical, sanitary and psychosocial relief. Discipline three consists of local and federal police forces. Discipline four consists of the necessary logistic support, and Discipline 5 consists of the communication teams.

Elia regularly organizes update conference calls during with the members of the management cell. If requested by the Federal Ministers of Energy and of Economy a physical meeting can be organized at the NCCN. The NCCN also regularly distributes situation reports to its crisis partners based on the information it receives from Elia.

3.1.10.1.5 Load shedding (complete and shortened procedure)

Not until Day D-1 between 4 pm and 7 pm, Elia can detect a probability of an actual shortfall for Day D. Elia will have the necessary information (e.g. production programs, import programs, estimate of consumption, etc.) from the market players to estimate whether or not an actual shortfall will occur on day D. When Elia notifies the detection of a probability of an actual shortfall, the Minister of the Interior can decide to activate the federal phase of the crisis management structure in order to manage the consequences on society. The population is therefore informed on the evening of Day D-1 of any possible activation of the manual load shedding plan and the affected areas. Load shedding is the measure taken in extreme cases when no other measures prove to be sufficient to avert an electricity shortfall. Up to the last moment, the Federal Ministers of Energy and of Economy can decide to recall that decision. For example when consumption has strongly declined due to the efforts made by citizens and enterprises.

3.1.10.1.6 Return to a normal situation (complete and shortened procedure)

As soon as Elia determines that no further action is needed, they inform the Federal Ministers of Energy and of Economy, the Minister of the Interior, the Regional Ministers of Energy, the Directors-General of the Directorate-General for Energy and of the National Crisis Center through the formal notification procedure. The decision to return to a normal situation will be made within the management cell and will be communicated to the crisis partners and the population. If the federal phase was applied, the federal phase will be lifted.

3.1.9.2. Procedure in case of Sudden Phenomena

In case of absence of control area adequacy for a certain period during day D, which is detected on Day D-1 after 7 pm, the procedure in case of an electricity shortfall cannot be activated. Instead, the transmission system operator (TSO) will use the measures of the System Defense Plan to prevent the propagation or worsening of an emergency state. This may include the application of manual or automatic load-shedding, without prior approval of the Federal Ministers of Energy and of Economy.

The application of defense measures in case of a late detection of an electricity shortfall gives substance to the requirement of the ministerial decree “Load-shedding Plan”, in which the TSO is requested to apply measures to protect the electricity system against “sudden phenomena” that could jeopardize the integrity of the system.

Chapter 7.6 of the System Defense Plan includes the order of measures that should be applied (if reasonably possible) prior to the activation of manual load-shedding:

1. Activation of reserves for balancing the system according to the applicable market rules
2. Application for inter-TSO assistance in the emergency state
3. Disconnection of electric accumulation heating and reduction of voltage in public distribution grid by 5%
4. Disconnection of pump storage plants operating in pump mode if not yet applied in step 1.

If the integrity of the system is still jeopardized, despite the application of the measures described above, the TSO could proceed to activate manual load-shedding to instantly reduce the electricity demand of a limited number of consumers for the time necessary and to avoid a further degradation of the electrical system.

The TSO informs the Federal Minister of Energy and the NCCN about the situation as soon as possible. The TSO notifies its stakeholders through multiple communication channels about the emergency state. TSO and DSOs publish the measures on their websites so that the grid users that will be disconnected will be informed as fast as possible about the period of disconnection to allow them to prepare themselves.

If a sudden phenomenon or the consequences of the supply interruption would lead to a national crisis there is a *Royal Decree of 31 January 2003 on the establishment of the contingency plan for crisis events and situations that require coordination or management at national level* on which the Minister of the Interior can decide to activate the federal phase of the crisis management structure in order to manage the consequences on society of the unforeseen supply interruption.

For the upcoming period, these principles need to be further developed and translated into a common procedure.

3.1.9.3. System Defence Plan

As mentioned in the previous chapter, Elia's System Defence Plan describes the automatic and manual measures intended to prevent blackouts, limit the spread of disruption and stabilise the grid during a state of emergency with a view to restoring a normal or alert state as quickly as possible with minimal impact on grid users. Elia compiled this document pursuant to the provisions of Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration (NC E&R) and to other network codes, the Royal Decree of 22 April 2019 establishing a federal technical regulation for the management of

and access to the electricity transmission system (the Federal Grid Code), other relevant legal provisions as well as any relevant local legislation.

Pursuant to NC E&R Article 6, section 1, when designing or reviewing their respective restoration plans all European TSOs must ensure consistency with the corresponding measures contained within the plans of other TSOs in their synchronous area as well as those of neighbouring TSOs belonging to another synchronous area. Such measures include the following as a minimum. Inter-TSO assistance and coordination in an emergency state, the frequency deviation management procedure (section 7.1) and the assistance for active power procedure. Coreso (the Regional Security Coordination Centre for Electricity) has drawn up a technical report on the consistency of the measures in 2019.

The table below provides a simplified overview of the defensive measures that can be enacted to return flows (including imports), voltage or frequency to within safe operational limits in real time as well as those measures to be enacted should a (potential) shortage be detected in advance. These measures are described in greater detail in the System Defence Plan that can be consulted on Elia's website.

Field Code Changed

			In the event of real-time incidents						In the event of a (risk of) shortage
			Current	Voltage		Frequency		Import	(generation + import) < load
			Too high	Too low	Too high	Too low	Too high	Too high	
POTENTIAL DEFENSIVE MEASURES	PGMs, HVDC, Storage	More MW injection into the grid	x			x		x	x
		Less MW injection into the grid	x				x		
		More MVAr injection into the grid		x					
		Less MVAr injection into the grid			x				
	Demand facilities, HVDC, Storage	More MW offtake from the grid	x				x		
		Less MW offtake from the grid	x			x		x	x
		More MVAr offtake from the grid			x				
		Less MVAr offtake from the grid		x					
	System operator	Disconnect a connection	x	x	x				
		Block transformer tap changers		x					
		Reduce voltage set point by 5%				x		x	x
		Disconnect electric storage heaters				x		x	x
		Activate shortage procedure							x
		Automatic demand disconnection				x			
		Inter-TSO assistance		x	x	x	x	x	x
		Manual demand disconnection	x	x				x	x

Table 6: Defensive Measures

3.1.9.4 Load Shedding Plan

As described earlier on, article 261 §4 of the Federal Grid Code establishes a legal basis for the Ministerial Decree of 3 June 2005 on the establishment of the load-shedding plan of the electricity

network in Article. In turn, the load-shedding plan as defined in this Ministerial Decree is embedded in the System Defence Plan, which finds it origin in articles 11 to 22 of the Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration (NC ER).

The current load-shedding plan can be activated both automatically, in the event of a sudden frequency drop on the high-voltage grid, or manually, for example as a last measure in case of an anticipated power shortage. This involves disconnecting DSOs' substations from the grid to keep the system balanced and prevent a general blackout across all of Belgium. If this plan is activated, various high-voltage substations belonging to a single load-shedding group will have to be disconnected simultaneously. The load-shedding plan for Belgium was updated in 2015 resulting in eight such groups, each of which corresponds to a capacity of between 500 and 750 MW. In total, they account for about 35 to 40% of total peak consumption. The updated load-shedding plan has been operational since 1 November 2015. The load to be disconnected within each group is proportionally distributed over 5 zones of Belgium, meaning that municipalities from different parts of the country can belong to the same group. A single municipality – or even street – may be supplied by different DSO substations that are not part of the same group. The load shedding plan may change further depending on specific factors, such as work on the distribution grid, etc. as well as pursuant to the requirements of the Commission Regulation (EU) 2017/2196.

Pursuant to article 261 §4 of the Federal Grid Code, the Minister of Energy devises the Load-Shedding Plan based on TSO proposals. The Load-Shedding Plan may contain the following measures:

1. The obligation for the TSO to:
    a. Interrupt some or all grid connections;
    b. Interrupt or modify interconnections with other networks within the control area.
2. The obligation for consumers (or certain categories of consumers) throughout the country or in certain parts thereof to reduce their offtake of electricity from the grid to within the set limits;
3. A ban on using electricity for certain purposes.

Pursuant to NC ER Article 11(5), the System Defence Plan comprises a manual demand disconnection procedure and an automatic low frequency demand disconnection (LFDD) system. As such, the Load-Shedding Plan is included as part of the System Defence Plan. Pursuant to the

'Load-Shedding Plan' Ministerial Decree, the Load-shedding Plan can be enacted in connection with the procedures listed below:

- The procedure protecting the grid from unexpected phenomena that undermine the integrity of the grid without warning;
- The procedure protecting the grid in the event of an announced shortfall or shortfall risk for a considerable, foreseeable or otherwise, period of time. In connection with the Load-Shedding Plan, demand disconnection can take place either automatically via Low Frequency Demand Disconnection (LFDD) or manually via the manual demand disconnection procedure.

The application of the Load-Shedding Plan in these procedures is described in more details in chapters 3.1.10.1, 3.1.10.2 and 3.1.10.3.

3.1.9.5 High Priority Significant Grid Users (HPSGUs)

Articles 259, 261 and 261 of the Federal Grid Code contains the national monitoring of the lists of significant grid users as identified in the System Defence Plan and the Restoration Plan. These national lists of significant grid users contain on one hand significant grid users important for grid management and grid security defined by the transmission system operator and on the other hand significant grid users in the interest of public order and safety defined through the implementation of the Risk Preparedness Regulation by the Competent Authority.

3.1.9.6 Demand Reduction Measures

The second annex of the System Defence Plan contains a list called “demand reduction measures”. This is a list of either voluntary or compulsory measures that can be communicated to the broad public, public transport companies and/or regular companies asking them to reduce their offtake of electricity during a certain time slot. It is based on a 2015 study done by Deloitte analysing possible measures and their impact on demand on the one hand but also on the other hand on safety and on levels of inconvenience. For example, it has been decided not to dim street lights due to safety concerns, but transport by train can be reduced to weekend schedules. In the case of the shortfall procedure, Elia can decide to ask the Minister of Energy to call for these demand reduction measures. An estimation has been made per measure what the impact would be in MW on total consumption. This list is updated each year and will be modernised to include the charging of electric vehicles and the use of heat pumps.

3.1.10. Business Continuity Plans

All of the main organizations active in the electricity supply either have developed solid business continuity plans (BCP) or are in the process of designing and implementing them. Conform the provisions in article 24 of Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation (SOGL), Elia has adopted a business continuity plan detailing its responses to a loss of critical tools, means and facilities, containing provisions for their maintenance, replacement and development. The National Crisis Center has also, developed a BCP. Finally, the Federal Public Service for Economy, SME's, Self-Employed and Energy will work on a BCP in 2021 based on existing BCPs.

The main goal of these BCPs is to define the critical business processes for each organization. Starting from a comprehensive list of activities, the possible scenarios for a discontinuity of their functioning were analyzed and those activities crucial for the continuity of the organizations were selected. The negative impact can be among others: financial, political, judicial and/or reputational. The activities could be related to IT, telecommunication, critical infrastructure, human resources, energy market functioning, etc.

After defining these critical processes, organizations will define a Recovery Time Objective (RTO) per process. This is the acceptable amount of time to restore a certain process. For example, for the Federal Public Service for Economy, SME's, Self-Employed and Energy, we will look at each of the scenarios defined in this risk preparedness plan and work out an RTO per process. This may vary quite heavily between scenarios and processes. Reflection on the timing implications of certain scenarios will play an important role in keeping the downtime to a minimum in the event of an emergency.

Business continuity management is one of the domains in risk preparedness that is never complete. We acknowledge the importance of further progress within the organizations involved in the electricity supply chain. Therefore we aim to review the situation every four years. These plans also need to be maintained and tested regularly; the critical processes must be confirmed or adjusted and the technical solutions and the organizational recovery procedures must be tested and verified. The current Covid-19 pandemic has also proven to be a good assessment of our existing resilience and has helped to show some shortfalls in our current business continuity capabilities.

3.1.11. Restoration Plan

Elia's Restoration Plan contains a range of measures that can be implemented in the wake of a serious disruption in view of restoring a normal state of the system following a state of emergency

or a state of blackout. System restoration comprises a sequence of coordinated measures that are prepared as much as possible in advance.

The Restoration Plan has been designed by Elia pursuant to the provisions of Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration (NC ER) and to other network codes, the Federal Grid Code, other relevant legal provisions (public health and safety, nuclear safety, etc.) as well as any relevant local requirements.

Elia activates those Restoration Plan procedures with a major cross-border impact in coordination with the affected TSOs.

Pursuant to NC ER Article 23(5), the Restoration Plan comprises three procedures:

- The re-energisation procedure;
- The frequency management procedure;
- The resynchronisation procedure.

The actual re-energisation procedures are based on the assumption that:

- no grid components were damaged or rendered unavailable as a result of the incident(s) that led to the blackout;
- there are sufficient numbers of well-trained personnel in the operational control centres;
- operators have an overview of the state of the system via the SCADA system;
- circuit breakers can be controlled remotely from the control centres.

In practice, one or more of these conditions may not be met. The measures in the actual restoration plan were designed without prejudice to other emergency measures applied by Elia to handle a crisis depending on the circumstances.

Pursuant to NC ER Article 6(1), when designing or reviewing their respective restoration plans all European TSOs must ensure consistency with the corresponding measures contained within the plans of other TSOs in their synchronous area as well as those of neighbouring TSOs belonging to another synchronous area. Such measures include the following: as a minimum the frequency management procedure and the top-down re-energisation strategy. Coreso (the Regional Security Coordination Centre for Electricity) performed a consistency check in 2019.

The measures of the restoration plan are described in greater detail in the document that can be consulted on Elia's website.

Field Code Changed

3.2. Communication mechanisms to inform the public

During a crisis, alerting and informing the population is crucial and is done through different communication channels: radio, TV, press releases, social networks of the authorities, etc. In Belgium, there is an additional communication tool specifically dedicated to alerting citizens in case of an emergency situation: BE-Alert.

Introduced by the National Crisis Centre and officially launched in June 2017, the BE-Alert platform can be activated at the municipal, provincial and federal level and uses different communication channels: voice calls on fixed phones or portables, SMS, e-mails, social media like Facebook and Twitter. This address-based system functions by selecting an area on a map and by sending a warning message to the people that previously registered their address via the BE-alert website.

Field Code Changed

In parallel, the National Crisis Centre has developed and implemented a mechanism based on location-based SMS to warn all the people that are present within a determined area, without any prior registration. This location-based system functions by selecting an area on a map and by sending a warning message to the mobile users identified by mobile operators. It has already been activated during numerous events. The activation procedure of Alert-SMS is integrated in the BE-Alert platform.

How to alert citizens in the event of a national crisis and which channels to select (traditional media, social networks, BE-alert,...) is an inherent part of the communication strategy that will be proposed by the Information Cell and approved by the responsible ministers. The federal crisis structure is further described in chapter four on the roles and responsibilities of the Crisis Coordinator.

On top of this, a specific website has been created by the crisis partners to be ready to inform the public in the case of an electricity crisis. It contains hidden pages with preventive measures and mitigations measures in case of an activation of the load-shedding plan or even in case of an electrical blackout. If deemed necessary, these pages are ready and can be online within short notice. Belgian media is highly acquainted to this website and will refer to it in their coverage.

3.3. Market-based measures

Being ideally located in the centre of Europe, Belgium has a highly interconnected electricity market. The internal functioning of the market is also well equipped to handle external and internal shocks in the system. To describe the market based measures that have been put in place in Belgium, we will focus on interconnectivity and on the functioning of the electricity markets.

Belgium is centrally located in between the large German and French energy markets. We also have interconnections with the Netherlands, Luxembourg and as of recently with the United Kingdom. Lately, two new projects have increased our interconnectivity: the underwater NEMO link with the United Kingdom and the ALEGrO link with Germany, each having a capacity of 1GW, or roughly combined 20% of our production capabilities. Added to the existing links, Belgium has already achieved the 2030 EU targets for the electricity interconnection level (+-5GW or 40% of peak demand). Through these connections we are also able to access more renewable energy than that we can produce with our limited renewable resources. Additionally, Elia, being operational in the German markets through Elia Grid International, is strategically ideally placed to optimise further market integration. Belgium is internationally connected through the ICE and the EPEXSPOT markets with advanced price coupling mechanisms.

Internally, Belgium has a robust electricity market: Forward markets, OTC, day ahead and intraday markets are available for market players. We also have a strong balancing market with balancing responsible parties, coordinated by Elia. The liquidity of the balancing markets is increasing year by year with more products and shorter bidding deadlines. Our Loss of Load Expectation (LOLE) is 3 hours (target set each year by our Federal Minister of Energy), one of the lowest in comparison to other EU countries.

Alongside our energy only market, we are in the process of designing a Capacity Renumeration Mechanism (CRM) to be able to deliver capacity from 1/12/2025 onwards. According to Belgian law, the nuclear power stations will close in 2025. Therefore additional capacity will have to be procured in the market. The bidding process for this CRM is planned to start in October 2021, accommodating enough time for additional ~~power plants to be built on time~~capacity to be contracted.

Combining a well-functioning energy market (both energy only and, whenever necessary a capacity ~~market~~remuneration mechanism) with a high interconnectivity, will allow Belgium to be ready for challenges ahead; integrating more and more intermittent renewables whilst keeping grid stability at a very high level even if/when emergency scenarios occur.

Commented [F1]: Our ? Belgian ? CWE ? European ?

Commented [F2]: Doel van de CRM is niet om centrales te bouwen, maar om voldoende capaciteit te contracteren voor bevoorradingszekerheid.

Commented [F3]: De CRM is een tijdelijke maatregel gericht op het opvangen van de kernuitstap. Hij moet dan ook worden uitgefaseerd.

Commented [F4]: De Belgische CRM is geen capacity market.

3.4. Regional and bilateral procedures and measures

The identification of the regional procedures and measures can be found in Annex 1. These regional measures and procedures were identified within a drafting team as part of the Pentalateral Energy Forum, Steering Group 2.

4. Crisis Coordinator

Pursuant to article 11(1)(d) of Regulation (EU) 2019/941 the role of Crisis Coordinator has been assigned to the Departmental Crisis Cell of the Federal Public Service for Economy SMEs, Middle Classes, and Energy, based on a proposal discussed within the "Risk Preparedness Stakeholder" Task Force, which is further described in chapter five. This crisis cell acts as the single point of

contact for the European Commission and other Member States in case of security of electricity supply issues.

This Departmental Crisis Cell consists of at least the following participants:

- Director-General of the Directorate-General for Energy or his representative;
- Head of the Strategic Coordination Unit or his representative;
- Head of the Gas & Permits Unit or his representative;
- Head of the Legal Coordination Unit or his representative;
- Employee within the Energy Monitoring and Electricity System Unit or his representative;
- Single Point of Contact of the Departmental Crisis Cell;
- Liaison officer of Elia or his representative;
- Liaison officer of Synergrid or his representative and
- Representatives of the Federal Ministers of Energy and of Economy or their representatives.

The Chairman of the Departmental Crisis Cell decides - based on the nature of the crisis, the information provided by Elia and Synergrid as well as other information originating from other information channels - which phase of the internal emergency plan must be announced. In accordance with the internal procedures of this phase, the necessary actions are taken.

Based on the assessment of the adequacy situation, network status and meteorological and other data both of the own bidding zone and the wider interconnected system, Elia can identify the need to activate the Shortfall Procedure or the Procedure in case of Sudden phenomena. Elia informs the government partners in accordance with the existing notification procedures.

In some cases (e.g. when activating the load-shedding plan in the event of a shortfall or a sudden phenomenon), the impact of a large-scale, long-term power supply cut on society and the operation of public services may activate the need for a national strategic coordination to mitigate the consequences of this emergency situation.

In this case, the electricity crisis is managed in accordance with the principles of crisis management implemented in Belgium and the federal phase of crisis management is triggered. This means that multidisciplinary strategic coordination takes place at the national level, under the leadership of the Minister of the Interior, and a series of crisis cells are activated. In this context, the Departmental Crisis Cell of the FPS Economy will be invited to take part in the Evaluation Cell. The figure below gives an overview of the actors involved in the federal crisis management structure.

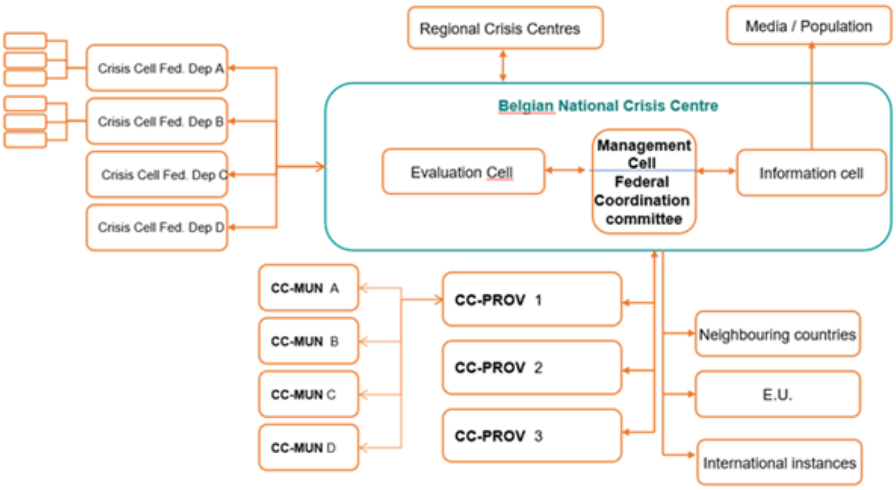

Figure 5: Federal Crisis Management Structure

The different cells displayed above have the following tasks :

- The Evaluation Cell is composed of experts with responsibilities for the security of electricity supply. It consists of at least the Departmental Crisis Cell of the FPS Economy, a representative of the transmission system operator and a representative of the distribution system operators (Synergrid). It is responsible for gathering the relevant technical information in order to assess the electrical situation and to monitor the electrical system. In addition, it provides technical advice to the Federal Coordination Committee.

- The Federal Coordination Committee (CC-Fed) brings together experts from various departments. It consists of at least representatives of federal services and departments related to operational disciplines (Civil Security, Public Health, Police, Defense, ...) and representatives of services and departments related to socio-economic sectors identified as particularly vulnerable in case of an electrical disruption (FPS Mobility, , FPS Economy, FPS Justice, Regional BIPT, Regional Crisis Centers, etc.). The CC-Fed's mission is to have a general overview of the situation (technical, socio-economic, international, information to the population...), to prepare strategic decisions and to follow up and coordinate the decisions taken by the ministers gathered in the Management Cell.

- The Management Cell gathers the ministers with direct responsibilities in the event of an emergency situation resulting from an electrical interruption. It makes the necessary

decisions and assumes responsibility for them. It also validates the communication strategy to inform the public.

- The Information Cell is composed of the spokespeople of the departments and ministers involved in crisis management. It is largely a reflection of the coordination committee. Its missions are to coordinate information to the population, assess the situation in terms of communication, formulate recommendations to the management cell and harmonize the communication of the various actors.

5. Stakeholder consultations

5.1 Consultation of stakeholders

To ensure a wide support, stakeholders were involved at the various stages of the elaboration of the draft Risk Preparedness plan. In this context a "**Risk Preparedness Stakeholder Task Force**" was created, composed of representatives of the following public and private organizations:

- The Directorate General for Energy;
- The National Crisis Center (NCCN);
- CREG, the Commission for Electricity and Gas Regulation;
- Elia, the Transmission System Operator for Electricity;
- Synergrid, the Federation of System Operators in Belgium;
- FEBEG, the Federation of Belgian Electricity and Gas Companies;
- Febeliec, the Federation of Belgian Industrial Energy Consumers;
- Test Achats – Test Aankoop, the Association for the Protection and Defense of Consumer Interests.

As such, the composition of the "Risk Preparedness Stakeholder Task Force" goes beyond the minimum requirements listed in Annex 1 of Regulation (EU) 2019/941.

The Task Force met at three occasions during the elaboration of the draft Risk Preparedness plans with special attention to the stakeholders' input concerning the identification of the national electricity crisis scenarios and the overall structure of the Risk Preparedness Plan. The figure below gives an overview of the different steps taken in an active stakeholder participation.

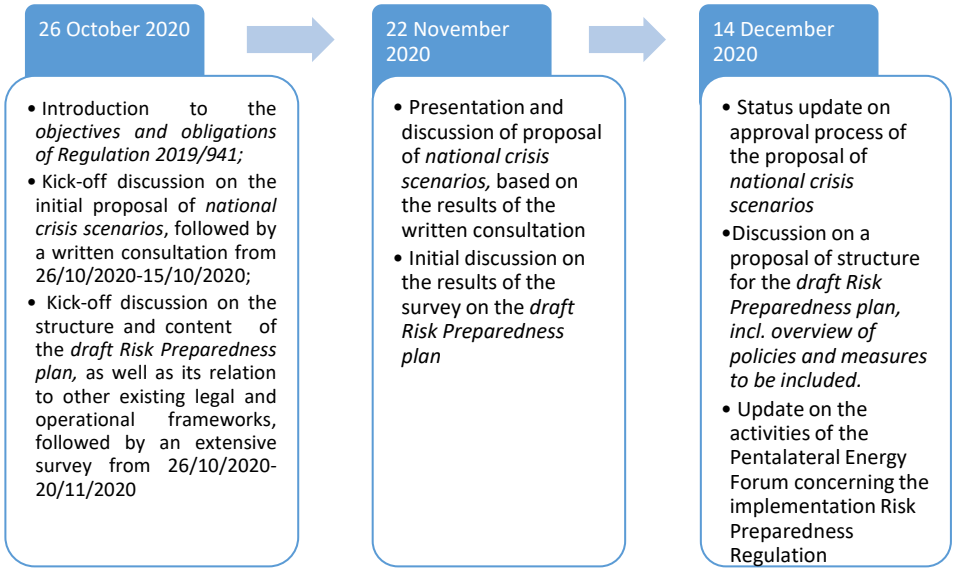

Figure 6: Timeline of the meetings of the "Risk Preparedness Stakeholder Task Force"

Through a digital survey, the stakeholders of the Task Force mentioned above were consulted on the overall structure and content of the draft Risk Preparedness Plan. It inquired about the following points:

- Legal status of the Risk Preparedness Plan;
- Relation and interaction with existing legal and operational frameworks;
- Required level of detail of the Risk Preparedness Plan;
- Views on the following topics: Regional solidarity, Crisis Coordinator, emergency tests and emergency communication tools.

The input that was received on the topics discussed above was used to create the overall structure and goals of the first draft of the Risk Preparedness Plan.

To further actively engage the stakeholders of the Task Force mentioned above, they were requested to select representatives to take part in a Risk Preparedness Drafting Team. From January 2021 to March 2021, the Risk Preparedness Drafting team digitally convened five times

to discuss the content of the different identified chapters. The following stakeholders had representatives taking part in the drafting team:

- The Directorate General for Energy;
- The National Crisis Center (NCCN);
- CREG, the Commission for Electricity and Gas Regulation;
- Elia, the Transmission System Operator for Electricity;
- Synergrid, the Federation of System Operators in Belgium;
- FEBEG, the Federation of Belgian Electricity and Gas Companies;

The Risk Preparedness Drafting Team convened on the topics shown in the figure below.

Figure 7: Risk Preparedness Drafting Team

Following the last Risk Preparedness Drafting Team meeting, all stakeholders that are part of the Risk Preparedness Stakeholder Task Force were invited to give comments on the draft between 16 March 2021 and 22 March 2021.

5.2 Consultation of the regional authorities

In parallel to the "Risk Preparedness Stakeholder Task Force", the energy administrations and cabinets of the Ministers of Energy of the Flemish Region, the Walloon Region and the Brussels-Capital Region (jointly "the regions") were actively informed during the monthly **CONCERE-ENOVER** meetings[5]. In addition, a topical meeting was organized on 30 November 2020. The CONCERE-ENOVER members were also given the opportunity to give their feedback on the initial proposal of *national crisis scenarios* and received the initial digital survey on the overall structure of the Risk Preparedness Plan. This allowed to collect their input and ensured consistency with the preventive and preparatory measures that are developed within the framework of the regional competences (e.g. mobility, water works).

Following the last Risk Preparedness Drafting Team meeting, representatives of the regions were invited to give comments on the draft between 16 March 2021 and 22 March 2021.

5.3 Regional consultation

The description of the process for the regional consultation can be found in Annex 1. This process was discussed within a drafting team as part of the Pentalateral Energy Forum, Steering Group 2.

5.4 Further consultations

In order to ensure consistency of risk-preparedness plans, competent authorities shall, before adopting their risk-preparedness plans, submit the draft plans, for consultation, to the competent authorities of the relevant Member States in the region and, where they are not in the same region, to the competent authorities of directly connected Member States, as well as to the ECG

Within six months of receipt of the draft risk-preparedness plans, the competent authorities referred to in paragraph 4 and the ECG may issue recommendations relating to the draft plans submitted pursuant to paragraph 4.

Within nine months of submitting their draft plans, the competent authorities concerned shall adopt their risk-preparedness plans, taking into account the results of the consultation pursuant to paragraph 4 and any recommendations issued pursuant to paragraph 5. They shall notify their risk-preparedness plans to the Commission without delay. The competent authorities and the Commission shall publish the risk-preparedness plans on their websites, while ensuring confidentiality of sensitive information, in particular information on measures relating to the prevention or mitigation of consequences of malicious attacks. The protection of the

[5] CONCERE-ENOVER is a coordination platform that strengthens the cooperation between the federal and regional governments in the field of energy, and brings together representatives of the four energy administrations and the four ministerial cabinets in charge of energy, the Belgian Permanent Representation to the European Union and the Directorate General for European Affairs of the Federal Public Service for Foreign Affair

confidentiality of sensitive information shall be based on the principles determined pursuant to Article 19. 8. The competent authorities shall adopt and publish their first risk-preparedness plans by 5 January 2022. They shall update them every four years thereafter, unless circumstances warrant more frequent updates.

6. Emergency tests

6.1 Regional emergency tests

The description of the process for the regional emergency tests can be found in Annex 1. This process was discussed within a drafting team as part of the Pentalateral Energy Forum, Steering Group 2.

6.2 National emergency tests

The question of organizing additional national emergency tests was part of the digital survey sent to the stakeholders and the regions, as discussed in more detail in chapter 5.1. All stakeholders agreed that it will be beneficial to organize national emergency tests alternating the regional emergency tests.

The national emergency tests will built further on the lessons learnt from the national crisis exercise organized in 2016, as well as the separate crisis exercises the different stakeholders organize separately. The national crisis exercise specifically focused on testing the Procedure in case of an electricity shortfall. The exercise was aimed at testing the detection of a possibility of an electricity shortfall. In concrete terms this means that the exercise was mostly aimed at testing the first steps of preparation as described in the common procedure, in chapter 3.1.9.1. Therefore, the active participants in this crisis exercise were:

- The Cabinet of the Minister of the Interior
- The Cabinet of the Federal Minister of Energy
- The Cabinet of the Federal Minister of Economic Affairs
- The Cabinet of the Minister of Energy of the Brussels-Capital Region
- The Cabinet of the Minister of Energy of the Flemish Region
- The Cabinet of the Minister of Energy of the Walloon Region
- The National Crisis Centre
- The Federal Public Service Economy
- Elia, the transmission system operator
- Synergrid, Federation of Electricity and Gas Operators in Belgium

The main goal of the exercise was to make the different stakeholders and partners aware of their specific role in the procedure, as well as analysing the information flow between the different partners and crisis cells involved.

After the exercise, a final evaluation report was established by the National Crisis Centre and the Directorate-General for Energy. Every Department, cell and actor involved took it upon themselves to act upon the recommendations following this exercise. Mid-April the next year, a follow-up Task Force convened to discuss and ensure the follow-up of the recommendations in the final report. Both this report and the active participants during this 2016 exercise will be the basis for the next national crisis exercise in light of the Risk Preparedness Plan.

The stakeholders agree that it will be beneficial to start organizing exercises with the core crisis partners, and enlarge this group over the course of the years. It is also stressed that the exercises can take place in various forms ranging from seminars and workshops over tabletop exercises to full-scale exercises.

Annex 1: Risk preparedness in the Pentalateral Energy Forum

The Penta Risk Preparedness Chapter will be added before the deadline for the draf plan.