



# Risk Preparedness Plan for the Electricity Sector

<b>Content</b>	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 a 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 Plan 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.
<b>Version</b>	Final 1.3
<b>Latest version</b>	12 January 2022
<b>Competent Authority</b>	Federal Minister of Energy
<b>Contact</b>	Be-riskpreparedness@economie.fgov.be
<b>Region</b>	Pentalateral Energy Forum (AT, BE, CH, DE, FR, LU, NL)

# Content

<b>CONTENT</b> .....	<b>3</b>
<b>LIST OF FIGURES</b> .....	<b>5</b>
<b>LIST OF TABLES</b> .....	<b>5</b>
<b>LIST OF ACRONYMS AND ABBREVIATIONS</b> .....	<b>6</b>
<b>1. INTRODUCTION</b> .....	<b>8</b>
1.1. CONTEXT RISK PREPAREDNESS PLAN .....	8
1.2. BELGIAN CONTEXT .....	9
1.3. REGIONAL CONTEXT .....	10
<b>2. SUMMARY OF THE ELECTRICITY CRISIS SCENARIOS</b> .....	<b>12</b>
2.1. REGIONAL ELECTRICITY CRISIS SCENARIOS .....	12
2.2. NATIONAL ELECTRICITY CRISIS SCENARIOS .....	14
2.2.1. Cyberattack on business-critical infrastructure .....	18
2.2.2. Physical attack .....	18
2.2.2.1 Physical attack on critical assets .....	18
2.2.2.2 Physical attack on control centres .....	19
2.2.3. Insider attack .....	19
2.2.4. Storm .....	19
2.2.5. Winter incident .....	20
2.2.6. Cold spell .....	20
2.2.7. Heavy precipitation and flooding .....	20
2.2.8. Dry period and heatwave .....	21
2.2.9. Pandemic .....	21
2.2.10. Loss of ICT tools and public telecommunication .....	21
2.2.11. Accidental violation of N-1 criterion due to a human error .....	22
2.2.12. Fuel shortage .....	22
2.2.12.1 Fossil fuel shortage .....	22
2.2.12.2 Nuclear fuel shortage .....	23
<b>3. ROLES AND RESPONSIBILITIES</b> .....	<b>24</b>
3.1. COMPETENT AUTHORITY .....	24
3.2. FEDERAL CRISIS STRUCTURE .....	24
3.3. CRISIS COORDINATOR .....	27
<b>4. PROCEDURES AND MEASURES IN THE ELECTRICITY CRISIS</b> .....	<b>28</b>
4.1. NATIONAL PROCEDURES AND MEASURES .....	28
4.1.1. Belgian NIS-Law .....	29
4.1.2. Belgian implementation EPCIP-Law .....	31
4.1.3. The Law of 11 December 1998 on the screening of personnel .....	32
4.1.4. Belgian National Adaptation Plan 2017-2020 .....	32
4.1.5. Federal Network Development Plan .....	34
4.1.6. Resilience of the network infrastructure .....	35
4.1.6.1 Resilience of the network infrastructure against potential storms and vortexes: .....	35
4.1.6.2 Resilience of the network infrastructure against heavy precipitation and flooding .....	36
4.1.6.3 Resilience of the network infrastructure against water shortage .....	36
4.1.6.4 Resilience of the network infrastructure against technical faults .....	36
4.1.7. Permits .....	37
4.1.7.1 Production permits for electricity .....	37
4.1.7.2 Transport permits for electricity .....	37
4.1.7.3 Sea cable Licenses .....	38
4.1.8. Test Plan .....	38

<b>4.1.9. Operational Procedures</b> .....	<b>41</b>
4.1.9.1 Procedure in the case of an Electricity Shortfall.....	43
4.1.9.1.1 Detection and notification.....	44
4.1.9.1.2 Preparation of the crisis consultation (complete procedure) .....	44
4.1.9.1.3 Informing the crisis partners and the population (complete and shortened procedure).....	45
4.1.9.1.4 Follow-up (complete and shortened procedure).....	45
4.1.9.1.5 Load shedding (complete and shortened procedure).....	45
4.1.9.1.6 Return to a normal situation (complete and shortened procedure).....	45
4.1.9.2 Procedure in the case of Sudden Phenomena.....	46
4.1.9.3 System Defence Plan .....	46
4.1.9.4 Load-Shedding Plan .....	47
4.1.9.5 High Priority Significant Grid Users (HPSGUs).....	48
4.1.9.6 Demand Reduction Measures.....	49
<b>4.1.10. Business Continuity Plans</b> .....	<b>49</b>
<b>4.1.11. Restoration Plan</b> .....	<b>50</b>
<b>4.1.12. Conclusion national measures and procedures</b> .....	<b>51</b>
<b>4.2. COMMUNICATION MECHANISMS TO INFORM THE PUBLIC</b> .....	<b>51</b>
<b>4.3. MARKET-BASED MEASURES</b> .....	<b>52</b>
<b>4.4. MARKET SUSPENSION CONDITIONS</b> .....	<b>53</b>
<b>4.5. REGIONAL AND BILATERAL PROCEDURES AND MEASURES</b> .....	<b>53</b>
<b>5. STAKEHOLDER CONSULTATIONS</b> .....	<b>54</b>
5.1. CONSULTATION OF STAKEHOLDERS .....	54
5.2. CONSULTATION OF THE REGIONAL AUTHORITIES.....	56
5.3. REGIONAL CONSULTATION .....	56
<b>6. EMERGENCY TESTS</b> .....	<b>57</b>
6.1. REGIONAL EMERGENCY TESTS .....	57
6.2. NATIONAL EMERGENCY TESTS .....	57
<b>ANNEX 1 : MEMORANDUM OF UNDERSTANDING ON RISK PREPAREDNESS</b> .....	<b>59</b>

## List of Figures

FIGURE 1: METHODOLOGY FOR IDENTIFICATION .....	15
FIGURE 2: TOPICAL GROUPINGS RISK SCENARIOS.....	17
FIGURE 3: FEDERAL CRISIS STRUCTURE .....	26
FIGURE 4: CRISIS COORDINATOR.....	27
FIGURE 5: OPERATIONAL PROCEDURES.....	42
FIGURE 6: COMPLETE SHORTFALL PROCEDURE .....	43
FIGURE 7: SHORTENED SHORTFALL PROCEDURE .....	44
FIGURE 8: HPSGU LISTS .....	49
FIGURE 9: RISK PREPAREDNESS DRAFTING TEAM .....	55

## List of Tables

TABLE 1: ENERGY POLICY RESPONSIBILITIES .....	10
TABLE 2: COMPETENT AUTHORITIES IN THE PENTA REGION .....	11
TABLE 3: PENTA-RATING OF ENTSO-E's 31 CRISIS SCENARIOS .....	12
TABLE 4: PENTA-RATING OF CRISIS SCENARIOS ACCORDING TO THEIR TOPICAL GROUPING.....	14
TABLE 5: NATIONAL ELECTRICITY CRISIS SCENARIOS.....	16
TABLE 6: OVERVIEW RISK PROFILE SCENARIOS .....	17
TABLE 7: MEASURES AND PROCEDURES.....	29
TABLE 8: CONSTRUCTION RELIABILITY-CLASS .....	36
TABLE 9: TEST PLAN .....	39
TABLE 10: DEFENSIVE MEASURES.....	47
TABLE 11: OVERVIEW MEASURES AND SCENARIOS .....	51

## List of acronyms and abbreviations

AREI/REGEI/GREI	General Regulation on Electrical Installations
BCP	Business Continuity Plan
BIPT	Belgian Institute for Postal Services and Telecommunications
Coreso	Coordination of Electrical System Operators <sup>1</sup>
CRM	Capacity Remuneration Mechanism
DG Energy	Directorate-General for Energy of the Federal Public Service Economy, S.M.E.s, Self-employed and Energy
DSO	Distribution System Operator
ECG	Electricity Coordination Group
EPCIP	European Program for Critical Infrastructure Protection
FPS	Federal Public Service
HPSGUs	High Priority Significant Grid Users
HTLS	High Temperature Low Sag
HVDC	High Voltage Direct Current
IPCC	Intergovernmental Panel on Climate Change
ISP	Information Systems Security Policy
LFDD	Low Frequency Demand Disconnection
NCCN	National Crisis Centre
NC DCC	Network Code on Demand Connection
NC ER	Network Code on Electricity Emergency and Restoration
NC HVDC	Network Code on High Voltage Direct Current Connections
NC RfG	Network Code on Requirements for Grid Connection of Generators
NIS	The European Network and Information System Security Directive
NRA	National Regulatory Authority
OSP	Operator Security Plan
RMI	Royal Meteorological Institute of Belgium
RTO	Recovery Time Objective

<sup>1</sup> <https://www.coreso.eu/about-us/our-mission/>

SCADA	Supervisory Control And Data Acquisition
SPOC	Single Point of Contact
TSO	Transmission System Operator

# 1. Introduction

## 1.1. Context Risk Preparedness Plan

The goal of the Risk Preparedness Plan for the electricity sector is to identify the possible risks related to security of electricity supply and to investigate whether the existing and planned measures sufficiently cover said risks. Pursuant to article 10, section 8 of the 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 (Risk Preparedness Regulation), the Risk Preparedness Plan shall be updated at least every four years, unless circumstances warrant otherwise. The document gives an overview of the national electricity crisis scenarios identified by the Federal Minister of Energy in her role as Competent Authority, as well as the relevant regional electricity crisis scenarios as identified within the Pentalateral Energy Forum. These electricity crisis scenarios serve as a starting point for the identification of existing and planned preventive, preparedness, and emergency response measures in order to prevent, prepare for and manage electricity crises, both on a national and on a regional level.

With this Plan, Belgium complies with the obligations of articles 10 to 12 of the Risk Preparedness Regulation. Under the supervision of the Competent Authority, the content of this Plan has been thoroughly discussed with the relevant stakeholders and the energy administrations of the Flemish, Walloon and Brussels-Capital Region, as is discussed in more detail in chapter six.

On a national level, the first version of the Risk Preparedness Plan aims to map the Belgian risk preparedness situation as it is today. By analysing whether the identified measures and procedures sufficiently cover the identified electricity crisis scenarios, it helps to highlight focus areas for the work to come over the next couple of years. While drawing up the Plan, the need to set a clear-cut definition of a crisis in national legislation was highlighted. Defining what constitutes a crisis pursuant to article 2, section 9 of the Risk Preparedness Regulation will be tackled in the revision of the relevant national legislation as discussed in chapter four.

In the aftermath of the floods of July 2021, which severely affected the energy infrastructure in the Province of Liège, an evaluation report was drafted and approved by the Task Force Crisis Management of the Directorate-General Energy (DG Energy) of the Federal Public Service Economy, S.M.E.s, Self-employed and Energy (FPS Economy). This report serves to identify action points for the crisis management plans and procedures of the different vectors. The identified action points for electricity crisis management will be dealt with in parallel to the action points that are highlighted in this Risk Preparedness Plan.

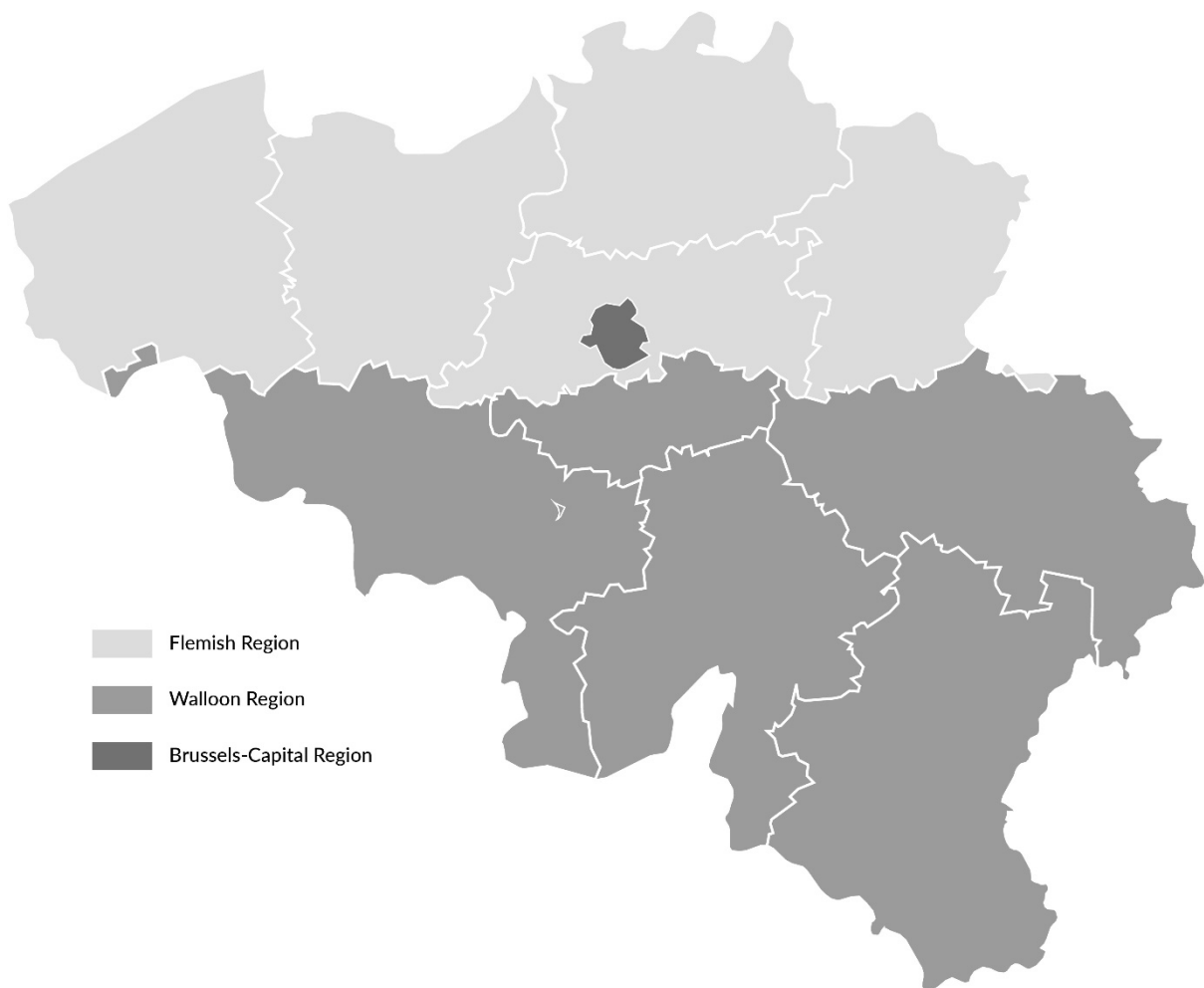
On a regional level, a Risk Preparedness Drafting Team within Steering Group II of the Pentalateral Energy Forum developed a common Risk Preparedness Chapter to be added to the national plans. It tackles the regional interpretation of the crisis scenarios, measures and procedures, coordination and the organisation of emergency tests. In addition to this, the same drafting team drew up a Memorandum of Understanding of the Pentalateral Energy Forum on Risk Preparedness in the Electricity Sector, which was signed during a Penta Ministerial meeting on 1 December 2021, and which was added to the annex of the national plans of the members of the Penta region. The Memorandum of Understanding further elaborates on the intent to develop common measures and procedures in case of regional electricity crises, on the intent to establish a common communication protocol, and on the intent to organise biannual regional crisis exercises.



## 1.2. Belgian Context

The Belgian governmental system consists of the Federal State, the Communities and the Regions.<sup>2</sup> Belgium has three communities that are based on the language that is spoken: the Flemish Community, the French Community and the German-Speaking Community. Apart from these Communities and the Federal State, Belgium also has three Regions: the Flemish Region, the Brussels-Capital Region and the Walloon Region. These Regions have legislative as well as executive bodies.

Energy policy responsibilities are divided between the Federal and Regional Governments by the Special Act for Institutional Reform of August 8, 1980. It is important to note, however, that the intra-Belgian institutional context on energy matters was changed by the Sixth State Reform with the Special Act of January 6, 2014. The table below gives an overview of the energy policy responsibilities of the Federal Government and of the Regional Governments.



---

<sup>2</sup> [https://www.belgium.be/en/about\\_belgium/government/federale\\_staet](https://www.belgium.be/en/about_belgium/government/federale_staet)

Table 1: Energy Policy Responsibilities

Federal Government	Regional Governments
Security of supply	Regulation of gas and electricity retail markets
National indicative investment plans for gas and electricity (in collaboration with the NRA)	Distribution and transmission of electricity (electricity grid <70Kv)
Nuclear fuel cycles + related R&D programmes	Distribution tariffs
Large stockholding installations	Public distribution of natural gas
Production and transmission/transport of energy (incl. Electricity grid >70Kv), incl. large storage infrastructure	District-heating equipment and networks
Transport tariffs and prices	New and renewable sources of energy (excl. nuclear)
Product norms	Recovery of waste energy from industry or other uses
Offshore wind energy	Promotion of the efficient use of energy

### 1.3. Regional Context<sup>3</sup>

The Pentalateral Energy Forum (Penta) is the framework for regional cooperation in Central Western Europe, consisting of Austria, Belgium, France, Germany, Luxembourg, The Netherlands, and Switzerland. The forum aims to work towards improved electricity market integration and security of supply. Jointly, Penta countries cover more than a third of the EU population and more than 40% of EU electricity generation. The initiative aims to allow energy policy to evolve from a purely national focus towards a regional approach. It allows political backing to a process of regional integration towards a European energy market. To this end, the Ministers for Energy of the Pentalateral countries regularly meet in order to discuss energy policy matters and give guidance on this regional cooperation. The work programme is implemented by the TSOs, ministries, regulatory authorities, and the market players who regularly meet in different support groups. This collaboration is formalized through the Memorandum of Understanding of the Pentalateral Energy Forum, signed on 6 June 2007 in Luxembourg.

Security of electricity supply has always been one of the most important pillars of the collaboration within the Pentalateral Energy Forum. To this end, at the beginning of 2020, the Forum received a mandate to work on a coordinated regional framework in light of the Risk Preparedness Regulation, while at the same time building further on its Memorandum of Understanding of 26 June 2017 on Emergency Planning and Crisis Management for the Power Sector. Penta therefore established a network of risk preparedness experts with representatives from ministries, regulatory authorities and TSOs within the framework of Support Group II, mainly focussing on security of supply. Competent authorities and their representatives, as depicted in the table below, actively contribute to the work.

<sup>3</sup> <https://www.benelux.int/nl/kernthemas/holder/energie/pentalateral-energy-forum>

The first two steps that were taken to work on this coordinated regional framework were the drafting of a common chapter that was added to the draft Risk Preparedness Plans and that was presented to the Electricity Coordination Group (ECG), and the signing of a Memorandum of Understanding of the Pentilateral Energy Forum on Risk Preparedness in the Electricity Sector. Both documents aim to provide an answer to the requirements pursuant to article 12 and 15 of the Risk Preparedness Regulation. The Memorandum provides a basis for the work that will be done in the following years on risk preparedness in the Penta region.

Table 2: Competent Authorities in the Penta Region

Country	Competent authority	Contact details
Belgium	Minister of Energy	<a href="https://www.belgium.be/en">https://www.belgium.be/en</a> Email: <a href="mailto:be-riskpreparedness@economie.fgov.be">be-riskpreparedness@economie.fgov.be</a>
Germany	Federal Ministry for Economic Affairs and Energy	<a href="https://www.bmwi.de/Navigation/EN/Home/home.html">https://www.bmwi.de/Navigation/EN/Home/home.html</a> Email: <a href="mailto:buero-iiic4@bmwi.bund.de">buero-iiic4@bmwi.bund.de</a>
France	Directorate General for Energy and Climate	<a href="https://www.ecologie.gouv.fr/">https://www.ecologie.gouv.fr/</a> Email: <a href="https://contact.ecologique-solidaire.gouv.fr">https://contact.ecologique-solidaire.gouv.fr</a>
Luxembourg	Minister for Energy	<a href="https://mea.gouvernement.lu/fr.html/">https://mea.gouvernement.lu/fr.html/</a> E-Mail: <a href="mailto:secretariat@energie.etat.lu">secretariat@energie.etat.lu</a>
Netherlands	Ministry of Economic Affairs and Climate Policy	<a href="https://www.rijksoverheid.nl/ministeries/ministerie-van-economische-zaken-en-klimaat">https://www.rijksoverheid.nl/ministeries/ministerie-van-economische-zaken-en-klimaat</a> Email: <a href="mailto:secretariaatelektriciteit@minezk.nl">secretariaatelektriciteit@minezk.nl</a>
Austria	Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology	<a href="https://www.bmk.gv.at/en.html">https://www.bmk.gv.at/en.html</a> Email: <a href="mailto:vi-8@bmk.gv.at">vi-8@bmk.gv.at</a>
Switzerland	Swiss Federal Office of Energy	<a href="https://www.bfe.admin.ch/">https://www.bfe.admin.ch/</a> Email: <a href="mailto:contact@bfe.admin.ch">contact@bfe.admin.ch</a>

## 2. Summary of the electricity crisis scenarios

### 2.1. Regional electricity crisis scenarios

As highlighted in the Risk Preparedness Regulation, regional crisis scenarios are an important element to identify and elaborate the precise scope for cross-border cooperation and assistance. Article 6 of the Risk Preparedness Regulation assigned the task of identifying regional scenarios to ENTSO-E. However, the report presented by ENTSO-E did not provide sufficient detail on certain scenarios and their particular relevance for specific regions. Therefore, the Penta Risk Preparedness Drafting Team saw the need to identify regional crisis scenarios pursuant to Article 5 and 6 of the Risk Preparedness Regulation, complementary to the work of ENTSO-E that had a more Pan-European perspective<sup>4</sup>. Penta voluntarily performed a much more detailed analysis along the same principles and applying the same ENTSO-E methodology for the Penta perimeter, through extensive exchanges among national experts, ENTSO-E and the European Commission.

Early in the process, national viewpoints among Penta countries were assessed in detail based on the national contributions to the ENTSO-E process. Despite a certain heterogeneity in levels of severity and ranking of scenarios, the assessment showed good correspondence and a significant cross-border dependency for a large majority of scenarios. Based on ENTSO-E's methodology for deriving a regional rating of crisis scenarios<sup>5</sup>, a Penta-rating of all crisis scenarios was established, as shown in the table below.

Table 3: Penta-rating of ENTSO-E's 31 Crisis Scenarios

#	SCENARIO	PENTA-RATING
1	Cyberattack - entities connected to the electrical grid	44.0
28	Heatwave	31.2
12	Winter incident	28.6
3	Physical attack - critical assets	27.2
17	Loss of ICT tools for real-time operation	25.2
10	Cold spell	22.8
29	Dry period	22.4
9	Storm	21.6
4	Physical attack - control centres	21.0
16	Multiple failures caused by extreme weather	20.8
6	Insider attack	20.2

<sup>4</sup> Cf ENTSO-E report from September 2020 "Risk-Preparedness Regulation – Identification of Regional Electricity Crisis Scenarios"

<sup>5</sup> See Appendix I of the Methodology to Identify Regional Electricity Crisis Scenarios in accordance with Article 5 of the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC.

18	Simultaneous multiple failures	19.4
24	Industrial/nuclear accident	19.4
5	Threat to key employees	19.0
11	Precipitation and flooding	18.4
27	Pandemic	18.0
19	Power system control mechanism complexity	17.2
20	Human error	16.6
13	Fossil fuel shortage	16.0
25	Unforeseen interaction of energy market rules	14.4
15	Local technical failure	12.6
7	Solar storm	12.2
2	Cyberattack - entities not connected to the electrical grid	11.2
26	Unusually big RES forecast errors	9.6
22	Serial equipment failure	9.0
31	Forest fire	8.6
21	Unwanted power flows	8.4
30	Earthquake	6.8
14	Nuclear fuel shortage	6.8
23	Strike, riots, industrial action	5.4
8	Volcanic eruption	3.2

Cyberattacks on entities physically connected to the electrical grid (i.e. grid operators, power plants or major (industrial) loads)) are consistently rated as the most relevant regional crisis scenario. A heatwave, a winter incident, a physical attack on critical assets, and the loss of ICT tools for real-time operation complete the top five.

Based on the table above that summarizes the severity and cross-border dependencies of crisis scenarios within the Penta region, it was agreed that the top five scenarios should receive particular attention for the elaboration of common measures. Notably, significant cross-border dependencies arise from the fact that Penta is characterized by high levels of integration and interconnectivity<sup>6</sup>, as well as coordination and cooperation among ministries, TSOs, regulators and market parties (in Penta and beyond), which leads to significant benefits, but also interdependencies when it comes to electricity crises. At the same time, integration and interconnectivity allows to manage risks through appropriate measures.

<sup>6</sup> As for market integration, note that Penta has been at the forefront of running a Flow-Based-Market Coupling regime. For instance, high levels of interconnectivity are demonstrated in the report of the Commission Expert Group on electricity interconnection targets "Towards a sustainable and integrated Europe".

During the assessment, experts also considered a more generic description of crisis scenarios, by using topical groupings. The specific scenarios may be less important for defining measures and arrangements than a more general type of scenario. For instance, whether an important line breaks down due to a storm or a heavy winter incident is hardly decisive in identifying the most suitable prevention and mitigation measures to ensure a safe balance between supply and demand at all times and locations.

For that reason, a Penta-regional rating of nine topical groupings was created by averaging the national ratings of all scenarios within a topical grouping, as shown in the table below.

Table 4: Penta-rating of Crisis Scenarios According to their Topical Grouping

SCENARIO BY TOPICAL GROUPING	PENTA-RATING
Cyberattack (# 1, 2)	27.6
Extreme weather (# 7, 9, 10, 11, 12, 16, 28, 29)	22.2
Physical attack (#3, 4, 5, 6)	21.9
Technical Failure (# 15, 17, 18, 22)	16.6
Other (# 19, 24, 26)	15.4
Fuel shortage (# 13, 14)	11.4
Market rules (# 21, 25)	11.4
Human-related (# 20, 23)	11.0
Natural disaster (# 8, 27, 30, 31)	9.2

Penta members agreed to consider the top three topical groupings as particularly relevant for its geographical perimeter in terms of impact, likelihood and cross-border dependency. Meanwhile, it was also agreed upon to not completely discard the rest of the list, as different measures of assistance may be applicable to a broader set of scenarios.

While discussing these three scenario groupings, Penta paid particular attention to triggers, the possible chain of events, and the impact those three scenario groupings would have on the electricity supply situation. While cyber-attacks could lead to corruption of control of the system (including the market), extreme weather conditions and physical attacks could result in immediate physical damage to infrastructure. At the same time, all of these scenarios can lead to operational impacts, structural or systemic degradation, and/or endanger security of supply through an uncontrolled mismatch of supply and demand. This can result in an electricity crisis with load shedding and blackout states, and has to be considered during the elaboration of the regional measures.

## 2.2. National electricity crisis scenarios

Pursuant to article 7 of the Risk Preparedness Regulation, the Belgian Competent Authority, the Federal Minister of Energy, identified 12 relevant national electricity crisis scenarios on 5 January 2021, after consulting the necessary stakeholders and considering the regional electricity crisis scenarios as defined in the ENTSO-E report of 7 September 2020.

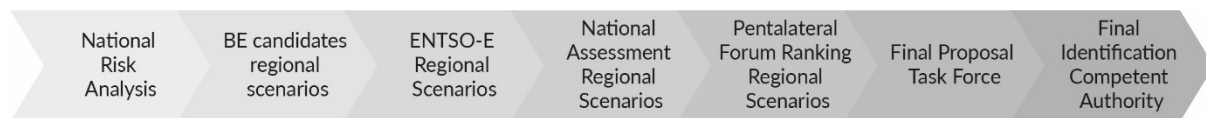
The identification of the national electricity crisis scenarios was based on a proposal discussed within the Risk Preparedness Stakeholder Task Force, which was established specifically for the purpose of the national implementation of the Risk Preparedness Regulation. The Task Force consisted of the necessary

stakeholders pursuant to article 7, section 2 of the Risk Preparedness Regulation, and is further described in chapter six that elaborates 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 crisis scenarios discussed during the process of identifying both the regional and national crisis scenarios. A first selection of scenarios was based on a national risk analysis performed by the National Crisis Centre (NCCN) in 2018. The 67 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 (TSO), the NCCN, and the DG Energy, these scenarios were analysed based on their probability and possible impact on security of electricity supply. In close collaboration with the relevant stakeholders, a more detailed method for the estimation of the likelihood and impact of the risk scenarios will be elaborated during the next risk preparedness cycle.

Pursuant to 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 TSO 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 identified scenarios were then further assessed based on their relevancy for 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 security of electricity supply. The likelihood as described for the different scenarios is in fact the likelihood that 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 that the cold spell would occur, but it is the likelihood that this cold spell would occur and lead to an electricity crisis. The likelihood was calculated by taking the sum of the likelihood of the actual event and the estimation by the TSO of the likelihood this event would lead to an electricity crisis.

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 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, since the main consequences will not solely impact 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.

Table 5: National Electricity Crisis Scenarios

#	SCENARIO
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. <sup>7</sup>
2a	Physical Attack on Critical Assets
2b	Physical Attack on Control Centres
3	Insider Attack
4	Storm
5	Winter Incident
6	Cold Spell
7	Heavy Precipitation & Flooding
8	Dry Period & Heatwave
9	Pandemic
10	Loss of ICT tools and Public Telecommunication
11	Accidental (unintended) Violation of N-1 Criterion due to a Human Error
12a	Fossil Fuel Shortage
12b	Nuclear Fuel Shortage

<sup>7</sup> This concerns the business-critical ICT infrastructure of all entities connected to the power grid that would have a substantial impact in case an uncontrolled interaction with the power grid caused by a cyberattack on the business-critical ICT infrastructure should occur.



Figure 2: Topical Groupings Risk Scenarios

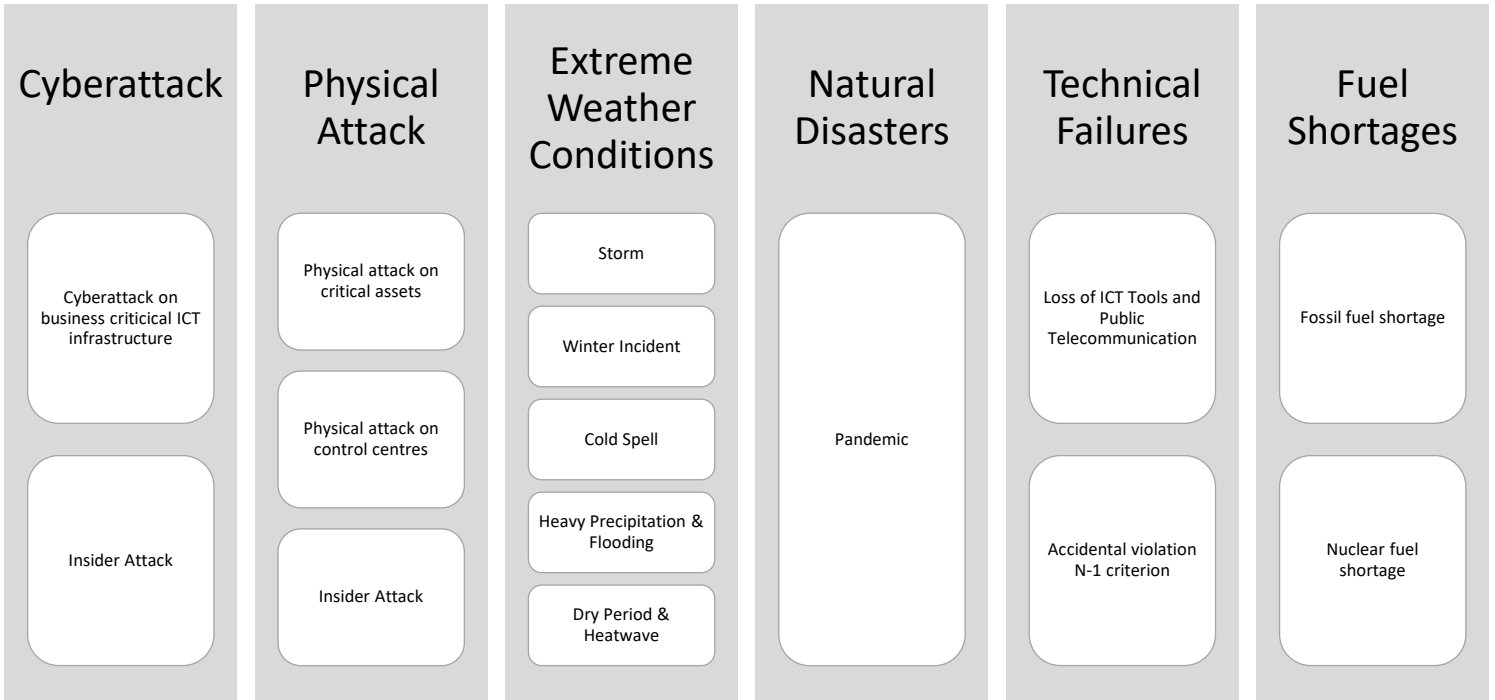


Table 6: Overview Risk Profile Scenarios

		Likelihood				
		Very Unlikely	Unlikely	Possible	Likely	Very Likely
Impact	Disastrous		3			
	Critical	12A	1, 2(A,B), 10			
	Major		11, 12B	5, 6, 7	4, 8	
	Minor			9		
	Insignificant					

### 2.2.1. 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 TSOs, distribution system operators (DSOs), 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 access to the attacked systems.

Assuming that the attacker(s) target(s) several systems simultaneously, the scenario was given an overall major risk profile, considering 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 the 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.

### 2.2.2. 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.

#### 2.2.2.1 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 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. 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.

### 2.2.2.2 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 TSOs, DSOs 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.

### 2.2.3. 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.

### 2.2.4. 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 regarding 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 built 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 fragilisation of the grid's integrity, impacting end users.

### 2.2.5. 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 fragilise the electrical network.

### 2.2.6. 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 combined 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.

### 2.2.7. 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 combined 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 fragilise the integrity of the grid, impacting 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.

### 2.2.8. 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 heatwave 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 characterised 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 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.

The scenario has a risk profile of major with a major risk of cross-border consequences. Statistical data proves the scenario to have a probability of likely, with a probabilistic estimation of having a major impact.

### 2.2.9. 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, for example, cause 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.

### 2.2.10. 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.

### 2.2.11. 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 TSO, 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.

### 2.2.12. 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.

#### 2.2.12.1 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 the case of fuel supply disruptions in Belgium, the TSO, 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 should 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.

### 2.2.12.2 Nuclear fuel shortage

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

The scenario of a nuclear fuel shortage involves the low stock or unavailability of fissile material to be used as fuel in nuclear power plants in combination with a high national electricity demand. As in the scenario of fossil fuel shortage described above, the nuclear supply or production can be interrupted due to various reasons, varying from technical issues, malicious attacks, sabotage, political or legal 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. Nonetheless, by the end of November 2021, the Government will reassess the Belgian situation in terms of security of supply and cost of electricity. If this monitoring shows that there is an unexpected security of supply problem, the government will take appropriate measures such as adapting the legal nuclear phase-out calendar for a capacity up to 2 GW. Taking into account the large share of nuclear power generation in the Belgian electricity mix, a probabilistic calculation estimates that a nuclear fuel shortage could have a major impact on the power system, although this impact is expected to decline in the near future.

On top of this, it is also estimated that a nuclear fuel shortage in Belgium would have a major cross-border impact. In the 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 considered 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.

## 3. Roles and responsibilities

### 3.1. Competent Authority

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

The Federal 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 strongly align with the tasks that were attributed to the Federal 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 September 2022. This designation is part of the general revision of the national legal and regulatory framework on electricity crisis management.

Furthermore, in accordance with article 3, section 3 of the Risk Preparedness Regulation, the following operational tasks regarding risk preparedness planning and risk management have been informally and provisionally delegated to the DG Energy of the FPS Economy:

- Participate in the 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;
- Organise 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.

### 3.2. Federal Crisis Structure

Every Federal Public Service of the Federal Government has its own Departmental Crisis Cell. In case of an electricity crisis, one of the leading roles will be played by the Departmental Crisis Cell of the FPS Economy, SMEs, Self-Employed and Energy. In case of an (imminent) electricity crisis, this Departmental Crisis Cell consists of at least the following participants:

- Director-General of the DG Energy or a representative;
- Head of the Strategic Coordination and External Relations Unit or a representative;
- Head of the Gas & Permits Unit or a representative;
- Head of the Legal Coordination Unit or a representative;
- Employee within the Energy Monitoring and Electricity System Unit or a representative;
- The Corporate Risk Manager of the FPS Economy, who will be the Single Point of Contact (SPOC)
- Liaison officer of Elia or a representative;
- Liaison officer of Synergrid or a representative and
- Representatives of the Federal Minister of Energy and the Federal Minister of Economy.



Based on the nature and the consequences of the electricity crisis, the composition of the Departmental Crisis Cell can be different and other participants than those listed above may be added. The chairperson of the Departmental Crisis Cell will depend on the type of crisis and the competences of the FPS Economy that are affected by the consequences of the crisis. In case of an electricity crisis, the chairperson of the Departmental Crisis Cell will be the Director-General of the DG Energy.

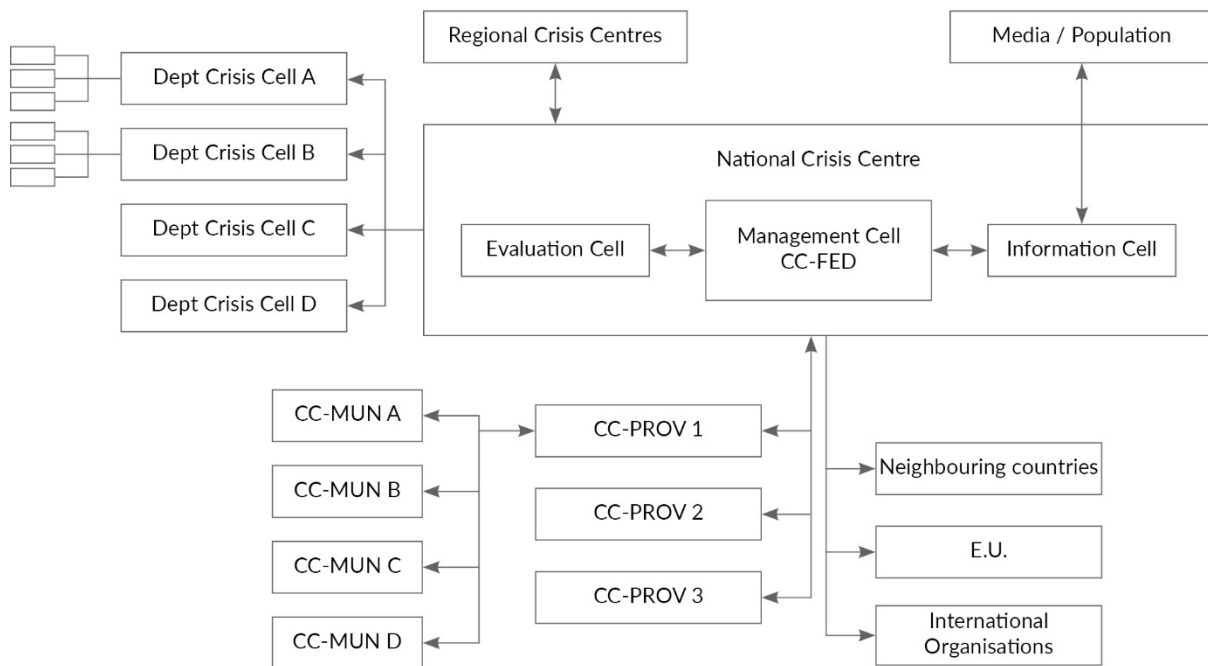
In case the consequences of the crisis affect large parts of the country, and have a significant effect on society, it is possible that the federal crisis phase will be activated by the Minister of the Interior. The Minister of the Interior will decide on a case-by-case basis whether strategic coordination at a national level is needed. This decision will be based on the guidelines for activating the federal crisis phase as described in the Royal Decree of 31 January 2003 on national emergency planning:

- Two or more Belgian Provinces are affected by the consequences of the crisis
- The resources needed, exceed the resources the Provincial Governor has available in his coordination task
- There is a threat of numerous victims
- There is a sudden occurrence or an imminent danger of major consequences for the environment and/or the food chain.
- There are violations or there is imminent danger of violations on the vital national interest or on the essential needs of the population
- There is a need for the implementation and coordination of different ministerial departments and federal institutions
- There is a need for general information to the public

While this version of the Risk Preparedness Plan was being drafted, the Royal Decree of 31 January 2003 was being revised by the NCCN.

Led by the Minister of the Interior, multidisciplinary strategic coordination will take place on a national level, and a series of crisis cells will be activated. In this context, the Departmental Crisis Cell of the FPS Economy will become part of the broader national crisis structure, and will be invited to take part in the meetings of the Evaluation Cell. In case the incident that caused the electricity crisis also triggered other crises, it is possible that several thematic evaluation cells are activated. The SPOC of the Departmental Crisis Cell of the FPS Economy may therefore need to attend several evaluation cells at the NCCN. The figure below provides an overview of the different actors involved in the federal crisis management structure.

Figure 3: Federal Crisis Structure



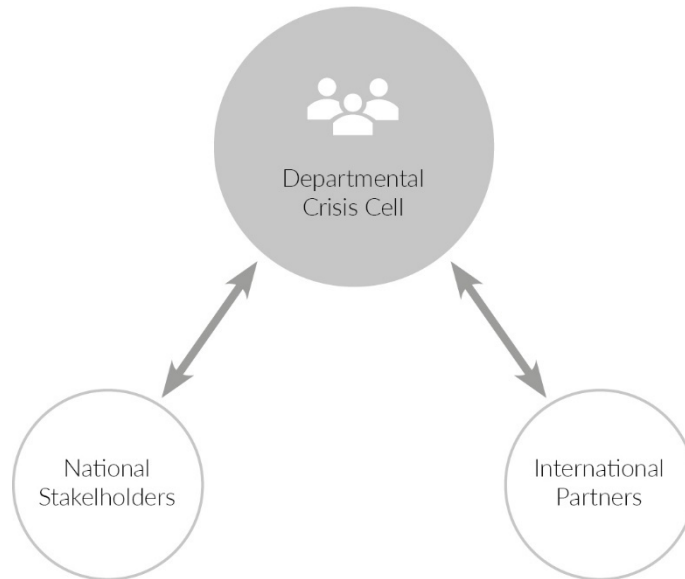
The different cells displayed above have the following tasks:

- **The Evaluation Cell** is composed of experts on security of electricity supply. It consists of at least the Departmental Crisis Cell of the FPS Economy, a representative of the TSO and a representative of the DSOs (represented through Synergrid). The evaluation cell is responsible for gathering the relevant technical information in order to assess and monitor the electrical system. Additionally, 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 the representatives of Federal Public Services and departments related to operational disciplines (Civil Security, Public Health, Police, Defence, etc.) and representatives of services and departments related to socio-economic sectors identified as particularly vulnerable in the case of an electricity crisis (Federal Public Service Mobility, Federal Public Service Economy, Federal Public Service Justice, Regional BIPT, Regional Crisis Centres, etc.). The Federal Coordination Committee's mission is to have a general overview of the situation (technical, socio-economic, international, information to the population, etc.), 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 electricity crisis. This cell decides on the necessary decisions and measures that need to be taken. It also validates the communication strategy of the Information Cell to inform the public.
- **The Information Cell** is composed of the spokespeople of the departments and Ministers involved in crisis management. Its missions are to coordinate information to the population, assess the situation in terms of communication, formulate recommendations to the Management Cell and harmonise communication of the various actors involved.

### 3.3. Crisis Coordinator

Pursuant to article 11, section 1,d, of the Risk Preparedness Regulation, the role of Crisis Coordinator has been assigned to the Departmental Crisis Cell of the FPS Economy, SMEs, Self-Employed and Energy, based on a proposal discussed within the Risk Preparedness Stakeholder Task Force, which is further described in chapter 6. The Departmental Crisis Cell acts as the SPOC for on the one hand the European Commission and the Members States, as well as other electricity neighbours, and on the other hand the national stakeholders involved. The contact details of the Crisis Coordinator can be found on the cover page.

Figure 4: Crisis Coordinator



## 4. Procedures and measures in the electricity crisis

### 4.1. National procedures and measures

The national electricity crisis scenarios, as identified in chapter 2.2, 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, definitions for three types of measures were established, pursuant to what is required in the Risk Preparedness Regulation. 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 the case of an Electricity Shortfall);
- **Emergency Response measures:** Measures that are in place, or that are planned, to mitigate the consequences of an electricity crisis.

Nevertheless, as can be seen in the table below, it is important to note that not all identified measures fit into one of these clear-cut definitions. For example, the Procedure in the 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.

Table 7: Measures and Procedures

Preventive	Preparedness	Emergency Response
Belgian NIS-Law		
Belgian EPCIP-Law		
Law on Security Clearances		
National Adaptation Plan		
Resilience of the Network		
Permits		
Federal Network Development Plan		
Test Plan		
	Shortfall Procedure	
	Sudden Phenomena Procedure	
	System Defence Plan	
	BCPs	
		Restoration Plan

Public Authorities
System Operators
All

#### 4.1.1. Belgian NIS-Law

Cyber Attack	Physical Attack	Insider Attack	Extreme Weather	Natural Disaster	Technical Failure	Fuel Shortage
✓		✓				

The European Directive 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), 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 (NIS Law). The Belgian NIS legislation is identified as a preventive measure for the cyberattack and insider attack scenarios. Its practical implementation is deemed to help mitigate the possible risks of the scenarios mentioned above occurring, as well as minimize the consequences connected to these types of scenarios.

The purpose of the NIS law is to establish a certain level of security of network and information systems, in order to ensure the continuity of so-called 'essential services'. Essential services are services that are crucial for the maintenance of critical societal and/or economic activities. To ensure the continuity of those services, operators of essential services must be able to prevent incidents or mitigate the consequences of incidents that affect the provision of these services, by taking appropriate measures to secure the network and information systems, from which the provision of the essential services depend.<sup>8</sup> By implementing the measures, audits and inspections as stipulated in the NIS law, the possibility of a successful insider attack also diminishes.

The Federal Minister of Energy has been designated as the sectoral authority for the energy sector and is responsible for, among other things, identifying the essential services and the operators of these essential services. Entities that meet the following criteria are considered to be operators of essential services:

- 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.

An exception to the above-mentioned identification methodology are the operators of a critical infrastructure.<sup>9</sup> 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 designated as an operator of essential services under the NIS Law.

Operators that are identified as essential service operators are notified as such by the sectoral authority, and must comply to the requirements of the NIS Law. These requirements are twofold:

- Protection of the network and information systems;
- Incident reporting and handling.

Concerning the protection of the network and information systems, the following steps are required:

- The operator must designate a SPOC for the security of its network and information system. The operator is required to communicate the most up-to-date contact details of this SPOC to the sectoral authority.
- The operator must make a description of its network and information systems.
- The operator must develop the necessary technical and organizational measures to manage security threats to the networks and information system. The operator must also develop measures to prevent incidents from happening and/or to mitigate the consequences of possible incidents that affect the security of the network and information systems. This in order to ensure the continuity of the provision of the essential service. These measures constitute the Information Systems Security Policy (ISP) and must meet the requirements of the ISO/IEC 27001 Information Security Management Systems Standard or an equivalent, subject to internal and external audits and inspections.
- The measures indicated in the operator's ISP are to be implemented.

---

<sup>8</sup> For the sake of legibility when referring to 'network and information systems, from which the provision of the essential services depend' the shortened version 'network and information systems' will be used.

<sup>9</sup> See 4.1.2 for information on 'critical infrastructure'

An operator of essential services is obliged to notify all incidents with significant consequences for the availability, authenticity, integrity or confidentiality of its network and information systems. A dedicated platform has been established for this incident reporting. An operator of essential services that has been affected by such an incident has the responsibility to handle the incident and to take the necessary reactive measures.

Under the guidance of the Federal Minister of Energy, the Federal Energy Administration has taken into consideration the different stakeholders of the electricity sector (producers, distributors, suppliers, traders, data analysts, etc.).

#### 4.1.2. Belgian implementation EPCIP-Law

Cyber Attack	Physical Attack	Insider Attack	Extreme Weather	Natural Disaster	Technical Failure	Fuel Shortage
	✓	✓				

The European Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, also referred to as “EPCIP” (European Program for Critical Infrastructure Protection) has been implemented in Belgian legislation through the Law of 1 July 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 measures and inspections that are carried out in light of the Belgian EPCIP-law are identified as preventive measures to mitigate the risks connected to the national electricity crisis scenario of a physical attack. By implementing these measures and inspections, the possibility of a successful insider attack also diminishes.

The NCCN is the point of contact in Belgium for the EPCIP-Law. The sectoral authority, the Federal 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 between 2015 and 2019. The law imposes a periodic re-valuation of critical infrastructures. This re-valuation is currently ongoing.

The operator of the critical infrastructures is notified of the decision and is required to implement internal 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 on 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 prioritisation of internal security measures. The OSP must make a distinction between permanent internal security measures which are constantly applied and gradual internal security measures which can be applied when necessary.

The critical infrastructures are subject to inspections by the sectoral authority in order to verify the proper implementation of the internal measures. The operator is required to organise 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 or based on an analysis provided by the federal police or security and intelligence services. If necessary, the major of the municipality where the critical infrastructure is located is also allowed to take additional external protection measures.

All parties concerned exchange relevant information to align all the protection measures taken.

#### 4.1.3. The Law of 11 December 1998 on the screening of personnel

Cyber Attack	Physical Attack	Insider Attack	Extreme Weather	Natural Disaster	Technical Failure	Fuel Shortage
		✓				

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

The Law of 11 December 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 other things, 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 Federal Minister of Energy. The National Security Authority is responsible for the coordination of the security investigations by the security and intelligence services.

#### 4.1.4. Belgian National Adaptation Plan 2017-2020

Cyber Attack	Physical Attack	Insider Attack	Extreme Weather	Natural Disaster	Technical Failure	Fuel Shortage
			✓			

The Belgian National Adaptation Plan for 2017-2020 proposed a set of national measures that focused on adaptation to climate change and its consequences. It was drafted by a working group within the National Climate Commission. The National Climate Commission was created in 2002 through a cooperation agreement between the federal state and the three regions. 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 2.2. 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](#).



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 2.2.

- 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 a 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 2.2, for example heatwaves, drought, and floods.

In this context, CORDEX.be<sup>10</sup>, presented its results in 2017. These identified 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 modelling. 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.be (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 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 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. Measure 6 will be discussed further as a federal adaptation measure, in close cooperation with the NCCN. Preparations on the analysis have started in October 2021.

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 neighbouring 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 organisation of different workshops.

---

<sup>10</sup> <http://cordex.meteo.be/meteo/view/en/19292661-+Cordex.be.html>

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 respect, more specifically, the consequences of scenarios related to extreme weather conditions. As this version of the Risk Preparedness Plan was drafted, preparatory meetings with the different stakeholders were being scheduled to start the work on a renewed National and Federal Adaptation Plan. As mentioned earlier on, a further elaboration of measure 6 will be on the agenda.

#### 4.1.5. Federal Network Development Plan

Cyber Attack	Physical Attack	Insider Attack	Extreme Weather	Natural Disaster	Technical Failure	Fuel Shortage
			✓			

The Federal Network Development Plan of the transmission system operator has a positive preventive impact on the risks concerning extreme weather conditions as identified in chapter 2.2. A more developed grid foresees required adequacy and security levels for withstanding disruptive events. 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 of 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 optimise the flows in that region. Although some have already been installed, further plans to optimise 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 optimise the current flows. On both borders, additional plans are being analysed in order to further optimise 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 realised. 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](#).

#### 4.1.6. Resilience of the network infrastructure

Cyber Attack	Physical Attack	Insider Attack	Extreme Weather	Natural Disaster	Technical Failure	Fuel Shortage
			✓			

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 2.2, in particular the risks related to extreme weather conditions.

##### 4.1.6.1 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 year of construction. The table below illustrates that a distinction is made between the construction classes in terms of reliability, with the reference windspeed at a height of 50 meters being provided for each class.

Over 70% of the 380kV network is built in accordance with the 1958 Royal Decree "1qb" while the other parts of the 380Kv network are in accordance with AREI/RGIE "2qb". For the other voltage levels the situation is more diverse. Their Construction reliability class strongly depends on the year of construction. The reference windspeed 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.

The time for repairs in case of damage will strongly depend on the intensity of the storm. For example, setting up an emergency overhead line will take up a minimum of about two weeks. When and if redundancy is available, other pathways will be used.

Table 8: Construction Reliability-class

From year 11	Construction reliability-class (CRC)		Wind at extreme loading [km/h] at 50m height
1920	Royal Decree		175
1931	Royal Decree + broken cable		172
1958	Royal Decree basic wind pressure "1qb"		149
1985	AREI/RGIE wind pressure "2qb"		184
2020	Design overhead line cfr. EN50341 - windspeeds: see EN1991	Reliability Level 1 - 70kV concrete poles	174
	Table 4.9 ANB: Extreme wind pressure $q_p(z)$ (N/m <sup>2</sup> ) $v_{b,0}$ : 26 m/s en $c_o = 1$ surface category II	Reliability Level 2 (New 70-110kV metallic & concrete towers)	191
		Reliability Level 3 (New 150, 220, 380kV towers)	206

#### 4.1.6.2 Resilience of the network infrastructure against heavy precipitation and flooding

The north of Belgium is located close to the estuaries of the rivers Scheldt and the Meuse. Key substations are in the immediate vicinity of those rivers. In the case of extreme floods, a scenario with a low probability, these substations are affected which can have a major impact. In light of the floods of the summer of 2021, which highly impacted the infrastructure in the Province of Liège, an analysis is being carried out to check where and whether extra preventive measures are needed and possible.

Control centres and data centres of the transmission system operator are in low-risk zones when it comes to flooding.

#### 4.1.6.3 Resilience of the network infrastructure against water shortage

Dry periods and low water levels across large parts of Europe can cause a 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, mutual assistance across borders might not be possible.

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

#### 4.1.6.4 Resilience of the network infrastructure against technical faults

The risk for unexpected outages of a series of infrastructure components of the same type is minimised 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

<sup>11</sup> 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.

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.

#### 4.1.7. Permits

Cyber Attack	Physical Attack	Insider Attack	Extreme Weather	Natural Disaster	Technical Failure	Fuel Shortage
	✓	✓	✓	✓	✓	

Although the application procedures connected to the approval of different types of permits, are not directly linked to the electricity crisis scenarios, it is identified as an added preventive layer for the different identified risks.

##### 4.1.7.1 Production permits for electricity

According to the Royal Decree of 11 October 2000 on the granting of individual licences for the construction of electricity generation plants, applications for production licences are submitted in fifteen copies by registered letter.

The application includes the following elements:

- Surname, first name, profession, place of residence and nationality of the applicant;
- In the case of the applicant being a company, the business name, the legal form, the registered office and, if applicable, its articles of association, as well as the documents confirming the competence of the signatories of the application;
- A proof of the technical capacity of the applicant, including previous experience, the references, diplomas and professional titles of the company's key executives, and an overview of the technical means envisaged for carrying out the work for the construction and operation of the installation;
- A proof of the economical capacity of the applicant, including the balance sheets and profit and loss accounts, the amount of own funds and the overall turnover and the capital/turnover and turnover/output ratios.

The Royal Decree of 11 October 2000 is currently being revised and will be replaced by a new Royal Decree.

##### 4.1.7.2 Transport permits for electricity

Permits for the use of the public domain to place electrical transport installations have to be granted pursuant to the Royal Decree of 26 November 1973, concerning the road permits referred to in the Law of 10 March 1925 on the supply of electricity.

This Royal Decree does not impose any requirements in the form of notifications to the authorities. De facto, 90 percent of the applications come from the TSO, of which all data is known. The remaining 10 percent come from offshore wind farms of power plant operators, of whom the data is known through other permits.

The Royal Decree of 26 November 1973 is also being revised as part of the amendment of the Law on administrative simplification and the deletion of the Electricity Supply Act of 10 March 1925. This planned amendment to the Royal Decree will, in the future, bring it more in line with the Royal Decree of 14 May 2002 on the permits for the transport of gaseous and other products via pipelines. In accordance with this Royal Decree of 14 May 2002, the application includes the following elements:

- The business name, the legal form, the registered office and, if applicable, its articles of association, as well as the documents confirming the competence of the signatories of the application;
- A proof of an administrative seat, of a principal establishment or of a registered office within a Member state of the Communities;

- A proof of the technical capacity of the applicant, including previous experience, references, diplomas and professional titles of the company's key executives, and an overview of the technical means envisaged for carrying out the work for the construction and the operation of the installation.

#### 4.1.7.3 Sea cable Licenses

Applications for sea cable licences shall follow the rules as established in the Royal Decree of 12 March 2000 on the detailed rules for the installation of cables entering the territorial sea or the national territory or being placed or used in the contest of the exploration of the continental shelf, the exploitation of its mineral resources and other non-living resources or the activities on artificial islands, installations or installations under Belgian jurisdiction.

The application has to be submitted in twelve copies and has to contain the following elements:

- Surname, first name, profession, place of residence and nationality of the applicant;
- If it concerns a company, the name of the company, its legal form, its registered office and, if applicable, its articles of association, as well as the documents confirming the competence of the signatories of the application;
- A proof of the technical capacity of the applicant, including previous experience, references, diplomas and professional titles of the company's key executives, and an overview of the technical means envisaged for carrying out the work for the construction and operation of the installation;
- A proof of economical capacity, including the annual accounts from the last three years, the balance sheets, equity, the overall turnover figure and the capital/turnover and turnover/result ratios;
- A proof of the existence of sufficient cover for the risk in terms of civil liability created by the installation, on the basis of criteria generally accepted by insurance companies.

#### 4.1.8. Test Plan

Cyber Attack	Physical Attack	Insider Attack	Extreme Weather	Natural Disaster	Technical Failure	Fuel Shortage
					✓	

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 such as the Network Code of Requirements for Grid Connection of Generators (NC RfG), the Network Code on Demand Connection (NC DCC) and the Network Code on High Voltage Direct Current Connections (NC HVDC). The Test Plan, as defined in article 43, section 2 of the NC ER, is identified as a preventive and preparedness measure mostly covering risks related to possible technical failures. The Test Plan describes the type of 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 brief 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 to article 43, section 2 of the Regulation (EU) 2017/2196.

Table 9: Test Plan

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 belong to 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 belong to 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 belong to 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 belong to 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

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
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.



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
(*) In case public DSOs, CDSO of SGUs are involved in these tools and facilities, they participate to this test.			

The most recent version of the Test Plan can be consulted on the [website of Elia](#). Pursuant to the Net Code Emergency and Restoration, the Test Plan has to be revised at least every five years, unless circumstances warrant otherwise. In Belgium, the Test Plan has to be approved by the Federal Minister of Energy. The most recent Test Plan was approved by the Federal Minister of Energy through the Ministerial Decree of 29 April 2021 for approval of the proposed Test Plan.

#### 4.1.9. Operational Procedures

In case the different preventive measures described in the chapters mentioned above are not sufficient to prevent the occurrence of the risks as identified in chapter 2.2, several operational procedures and plans 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 current 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 Ministerial Decree on the Load-Shedding Plan).

The Federal Grid Code of 22 April 2019, specifically article 261, section 4, creates a legal basis for the Ministerial Decree of 3 June 2005 on the Load-Shedding Plan. In turn, the Load-Shedding Plan as defined in this Ministerial Decree, is embedded in the System Defence Plan, which finds its 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).

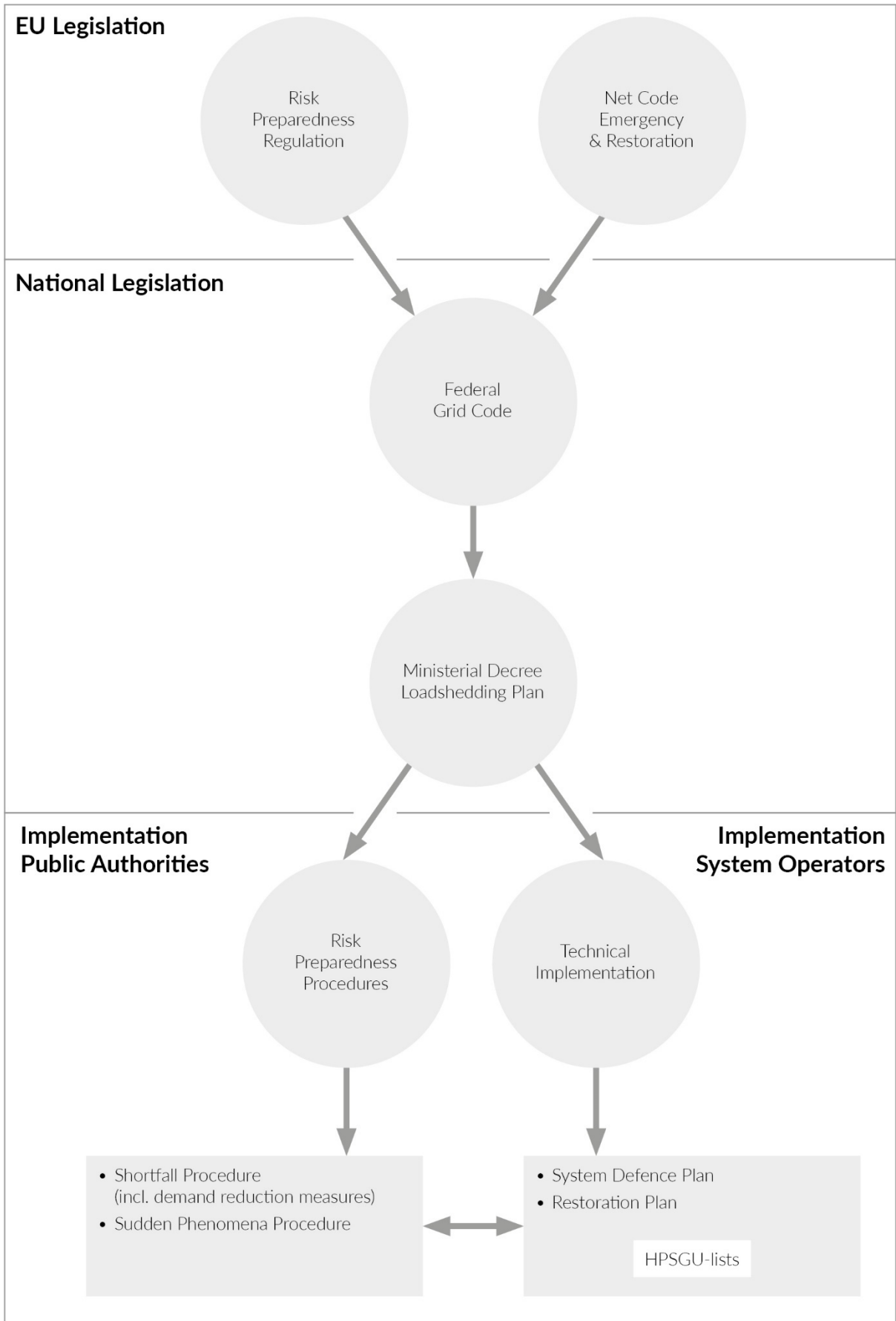
The TSO, Elia, has developed a global Load-Shedding Plan that can either be activated automatically in the event of an incident on the high-voltage network or that can be activated manually in the event of an electricity shortfall. The measures to restore an imbalance on the electrical system vary considerably 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 drafting of this version of the Risk Preparedness Plan, a review of the Ministerial Decree of 3 June 2005 on the Load-Shedding Plan, as well as the Federal Grid Code, taking into account the requirements of the Risk Preparedness Plan, was ongoing. The revision of the national regulatory and legal framework on electricity crisis management is foreseen to be completed by September 2022.

The schematic below provides an overview of the relevant legislation, the different measures as well as the different actors involved.

Figure 5: Operational Procedures



#### 4.1.9.1 Procedure in the case of an Electricity Shortfall

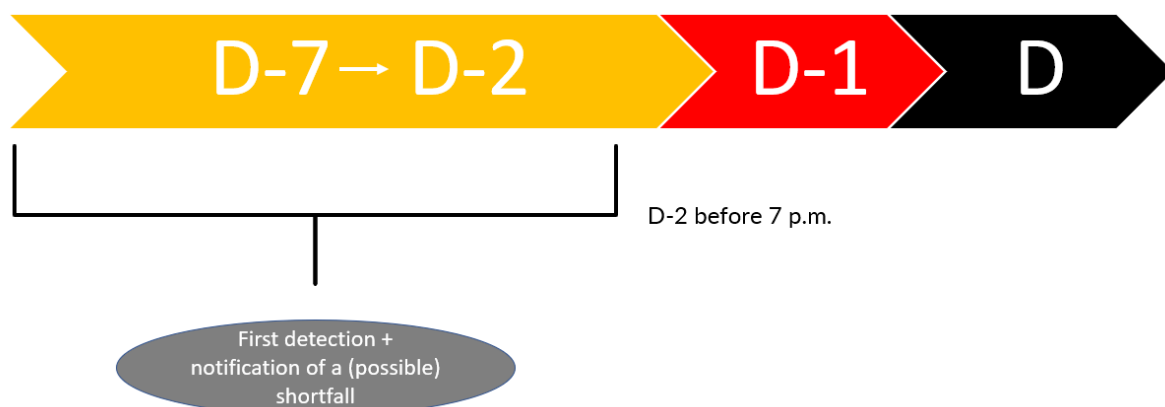
Cyber Attack	Physical Attack	Insider Attack	Extreme Weather	Natural Disaster	Technical Failure	Fuel Shortage
✓	✓	✓	✓	✓	✓	✓

In order to manage an expected electricity shortfall, a common procedure has been developed by the DG Energy of the FPS Economy and the NCCN, in close cooperation with the TSO, Elia, and the Federation of Electricity and Gas Operators in Belgium, Synergrid. The procedure is identified as a preparedness and emergency response measure for all identified electricity crisis scenarios. The Procedure in the case of an Electricity Shortfall (the Shortfall Procedure) aims to coordinate the actions of the crisis partners mentioned above on the following aspects:

- Notification of a possible shortfall and notification of an actual shortfall;
- Taking actions to maintain and/or restore the balance of the control area or reduce local energy shortages and;
- Preparing for a possible activation of the Load-Shedding Plan and the possible consequences thereof.

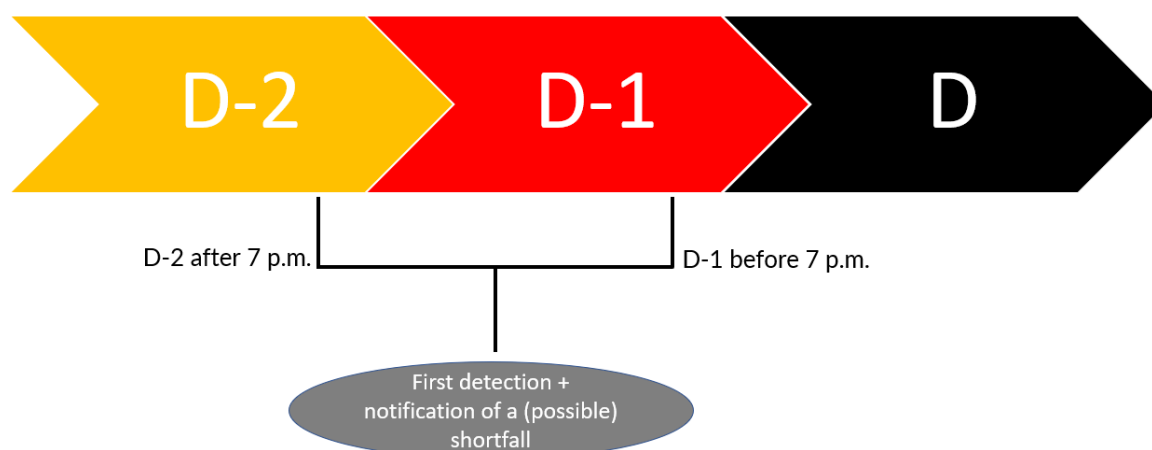
This procedure is based on the principles of relevant national legislation, the federal crisis management structure as discussed in chapter three, the involvement of various actors of the crisis cells, and the information on which Elia can take decisions. Based on the moment on which Elia detects and 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 detects and notifies 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 visualises the scope of the complete Shortfall Procedure.

Figure 6: Complete Shortfall Procedure



However, in case Elia detects and notifies a threat of a shortfall between Day D-2 after 7 pm and Day D-1 before 7 pm, the shortened Shortfall Procedure will be activated, since there is not enough time left to go through the complete Procedure. The schematic below visualises the scope of the shortened Shortfall Procedure.

Figure 7: Shortened Shortfall Procedure



#### 4.1.9.1.1 Detection and notification

Elia can detect a threat of a shortfall by analysing:

- 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 Minister of Energy
- The Minister of the Interior;
- The Regional Ministers of Energy and;
- The Directors-General of the DG Energy and the DG of the NCCN.

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. During the technical briefing, Elia gives more information on the following elements:

- The cause;
- The estimated impact of the shortfall;
- The expected duration;
- The size of the shortfall 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.

When the shortened Procedure is applied, there is no time for a technical briefing. In this case, the NCCN invites all members of the Crisis Cell for the first crisis consultations.

#### 4.1.9.1.2 Preparation of the crisis consultation (complete procedure)

As a first step, before the crisis consultation at the NCCN takes place, the FPS Economy convenes the members of their Departmental Crisis Cell. One of the tasks of this Departmental Crisis Cell is to analyse 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. At the same time, 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. The members will analyse the consequences of the situation on individual and collective security and will 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.

#### 4.1.9.1.3 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 planned measures. 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”<sup>12</sup> 1 to 4, containing:
  - The emergency call centres 100 and 112;
  - The Federal Public Service Health;
  - The Directorate of the Operations of Administrative police (DAO) of the Federal Police;
  - Civil Protection and the Ministry of Defence,
- Other relevant ministers and their departmental crisis cells and;
- The Belgian Institute for Postal Services and Telecommunications (BIPT).

#### 4.1.9.1.4 Follow-up (complete and shortened procedure)

Elia regularly organises update conference calls with the members of the Management Cell. If requested by the Federal Ministers of Energy and of Economy, a physical meeting can be organised at the offices of the NCCN. The NCCN also regularly distributes situation reports to its crisis partners based on the information it receives from Elia.

#### 4.1.9.1.5 Load shedding (complete and shortened procedure)

It is not until Day D-1 between 4 pm and 7 pm that Elia can actually confirm the probability of an actual shortfall for Day D. Only then Elia will have the necessary information (e.g. production programmes, import programmes, estimate of consumption, etc.) from the market players. 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. The population is 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.

#### 4.1.9.1.6 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 of Economy and of the Interior, the Regional Ministers of Energy, the Directors-General of the DG Energy and the DG of the NCCN 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

---

<sup>12</sup> Every emergency situation will be mitigated by different teams of people. In Emergency Planning there are five different Disciplines that work together 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.

partners and the population. If the federal phase was applied, the federal phase will be lifted, according to the procedures of the NCCN.

#### 4.1.9.2 Procedure in the case of Sudden Phenomena

In the case of absence of control area adequacy for a certain period of time during day D, which is detected on Day D-1 after 7 pm, the Procedure in the case of an Electricity Shortfall cannot be activated. Instead, the TSO will use the measures of the System Defence 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 defence measures in the case of late detection of an electricity shortfall is a condition for the application of the Ministerial Decree on the Load-shedding Plan, in which the TSO is requested to apply measures to protect the electricity system against sudden phenomena that could jeopardise the integrity of the system.

Chapter 7.6 of the System Defence 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 one.

If the integrity of the system is still at risk, 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, in order to avoid further degradation of the electrical system.

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

If a sudden phenomenon and its consequences lead to a national crisis, the Royal Decree of 31 January 2003 on the establishment of contingency plans for crisis events that require coordination or management at a notional level, will allow the Minister of the Interior to activate the federal crisis management phase. More specific conditions on the activation of the federal crisis management phase are described in chapter three.

During the drafting of this version of the Risk Preparedness Plan, a working group on the procedure in case of sudden phenomena was established. The goal of this working group is to work out a common procedure based on the principles described above, and in line with the Shortfall Procedure. These discussions will involve at least the NCCN, the DG Energy of the FPS Economy, the TSOs and Synergrid representing the DSOs.

#### 4.1.9.3 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 ER) and to other network codes, the Federal Grid Code, other relevant legal provisions as well as any relevant local legislation.

Pursuant to NC ER 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 taken to return flows (including imports), voltage or frequency to within safe operational limits in real time as well as those measures to be taken 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](#).

Pursuant to the network code on emergency and restoration, the plan needs to be revised at least every five years, unless circumstances warrant otherwise. As described above in the description of the Test Plan, the System Defence Plan proposed by the TSO, needs to be approved by the Federal Minister of Energy.

Table 10: Defensive Measures

			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 in to the grid	X			X		X	
		Less MW injection in to the grid	X				X		
		More MVAR injection in to the grid		X					
		Less MVAR injection in to 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		

#### 4.1.9.4 Load-Shedding Plan

As described above, article 261, section 4, of the Federal Grid Code establishes a legal basis for the Ministerial Decree of 3 June 2005 on the Load-Shedding Plan. In turn, the Load-Shedding plan as defined in this Ministerial Decree is embedded in the System Defence Plan, which finds its 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 the 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 correspond 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 five zones in 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 will 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 (NC ER).

Pursuant to article 261, section 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 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, section 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 Ministerial Decree on the Load-Shedding Plan, the Plan can be enacted in connection with the procedures listed below:

- The procedure protecting the grid from sudden 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 via the manual demand disconnection procedure.

The application of the Load-Shedding Plan in these procedures is described in more detail in chapters 4.1.10.1, 4.1.10.2 and 4.1.10.3.

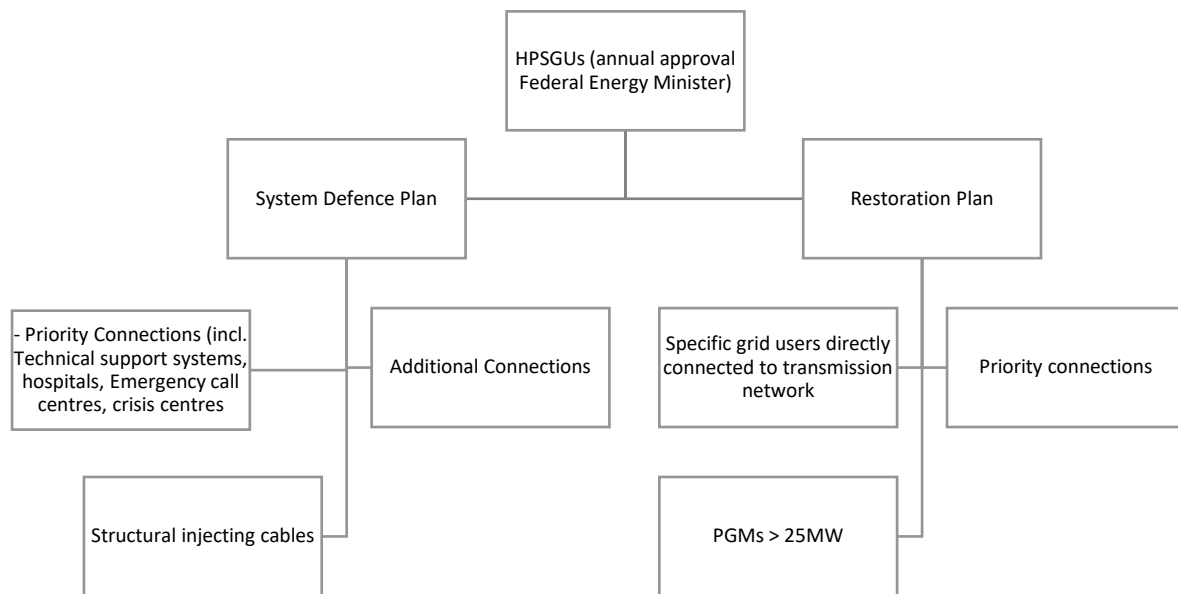
#### 4.1.9.5 High Priority Significant Grid Users (HPSGUs)

Articles 259, 261 and 262 of the Federal Grid Code contain the outlines of the process for ministerial approval of the lists of significant grid users and the high priority significant grid users as identified in the System Defence Plan and the Restoration Plan. The national lists of high priority significant grid users contain on one hand high priority significant grid users important for grid management and grid security defined by the TSO and on the other hand high priority significant grid users in the interest of public order and safety defined through the implementation of the Risk Preparedness Regulation by the Competent Authority.

The schematic below gives an overview of the types of users that are identified in the HPSGU list of the System Defence Plan on the one hand, and the HPSGU list of the Restoration Plan on the other hand. Both lists are approved by the Federal Minister of Energy on an annual basis.



Figure 8: HPSGU lists



#### 4.1.9.6 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 public, public transport companies and/or other businesses 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 and on the other hand on safety and 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 Federal Minister of Energy to call for these demand reduction measures. An estimation on the impact has been made to measure what the impact would be in MW on the total consumption. This list is updated annually and will include charging electric vehicles and the use of heat pumps. While the latest version of this Risk Preparedness Plan was drafted, a revision of the analysis of the list of possible demand reduction measures was ongoing.

Depending on the severity of the shortfall, some of the measures can be installed on a mandatory basis while others are used for sensitizing the public. For example, the Federal Minister of Energy could ask the public not to use saunas and jacuzzies from 5 p.m. to 8 p.m. during certain days of the week. Another example would be to ask advertising companies to not use neon light publicity for a certain period of time. Dormant ministerial decrees are in place to ensure the swift implementation of the demand reduction measures if needed.

#### 4.1.10. Business Continuity Plans

The stakeholders as described in the chapter on consultations, have either developed solid business continuity plans (BCP) or are in the process of designing and implementing them. In accordance with 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 NCCN has also developed a BCP. Finally, the FPS Economy will start working on a BCP in 2021 based on existing BCPs and information shared by the NCCN.

The main goal of these BCPs is to define the critical business processes for each organisation. Starting from a comprehensive list of activities, the possible scenarios for a discontinuity of their functioning

were analysed and those activities crucial for the continuity of the organisations 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, organisations 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 FPS Economy, each of the scenarios defined in this risk preparedness plan will be taken into account and an RTO per process will be established. 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 organisations 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 organisational 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.

#### 4.1.11. Restoration Plan

Elia's Restoration Plan contains a range of measures that can be implemented in the wake of a serious disruption, in order to restore a normal state of the system following a state of emergency or a state of black-out. System restoration comprises a sequence of coordinated measures that are, as much as possible, prepared 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. Similar to the Test Plan and the System Defence Plan, the proposed Restoration Plan by the TSO needs to be approved by the Federal Minister of Energy.

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

Pursuant to NC ER article 23, section 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, 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, 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](#).

#### 4.1.12. Conclusion national measures and procedures

In conclusion, the different preventive, preparedness and emergency response measures that were identified and described in the previous chapter, cover most of the identified scenarios. It is important to note that these measures can change and will adapt to changing legislation, both on an EU and a national level, as well as adapt to changing circumstances.

The table below gives a summary of how the scenarios are covered by the different identified measures and procedures. Two cases deserve some extra explanation. Firstly, the table below shows that at the moment the topical grouping of “natural disasters” is not covered by any preventive measures. This statement needs some nuance, since this group is at the moment only composed of the scenario of a pandemic. During the discussions with the stakeholders on the identification of the crisis scenarios, it was highlighted that typically for a pandemic the nature of the illness can vary widely. This makes it almost impossible to work with a fixed set of preventive measures. It is important to note, however, that the Covid-19 crisis had no significant impact on the security of electricity supply, which in this case was also partly due to the business continuity plans already in place.

A second case that deserves some more explanation are the preventive measures for fuel shortage, both fossil and nuclear. It is shown in the table below that these are covered by preventive measures, although these were not specifically mentioned in this Risk Preparedness Plan. Within the DG Energy of the FPS Economy the crisis management teams for oil, gas and nuclear infrastructure also established crisis procedures which contain preventive measures. On top of this, as is mentioned in the introduction, the Risk Preparedness Plan serves to highlight areas that deserve some extra attention over the next couple of years. Cross-vector emergency planning is one of them. Within the DG Energy a Task Force crisis management was established that aims to streamline the different crisis management procedures, and aims to organize joint crisis exercises. Apart from the public authorities, the network operators will also aim to continue to work on a more integrated policy.

Table 11: Overview Measures and Scenarios

	Cyber Attack	Physical Attack	Insider Attack	Extreme Weather Conditions	Natural Disaster	Technical Failure	Fuel Shortage
Preventive Measures	✓	✓	✓	✓		✓	✓
Preparedness Measures	✓	✓	✓	✓	✓	✓	✓
Emergency Response Measures	✓	✓	✓	✓	✓	✓	✓

## 4.2. 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 the case of an emergency situation: BE-Alert.

Introduced by the NCCN 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, and 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 who previously registered their address via the [BE-alert website](#).

In parallel, the NCCN has developed and implemented a mechanism based on location-based SMS to warn all the people who 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, etc.) is an inherent part of the communication strategy that will be proposed by the Information Cell and approved by the responsible ministers.

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 mitigation measures in the case of an activation of the Load-Shedding plan or even in the case of an electrical black-out. If deemed necessary, these pages are ready and can be posted online within short notice. Belgian media is well acquainted with this website and will refer to it in their coverage.

### 4.3. Market-based measures

Being located in the centre of Europe, Belgium has a highly interconnected electricity market. The internal functioning of the market is well equipped to handle external and internal shocks in the system. To describe the market-based measures that have been put in place, 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. 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 present renewable resources. Additionally, Elia, being operational in the German markets through 50Herz, is strategically placed to optimise further market integration. Belgium is internationally connected through the ICE and the EPEXSPOT markets with advanced price coupling mechanisms.

Belgium has a robust national electricity market: Forward markets, Over the Counter trading (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. Unlocking the flexibility potential on the consumer side requires further upgrading of the market design and the development of new digital tools and real-time communication platforms.

More strategically, an anticipative and recurrent mechanism is in place in Belgium for defining the adequacy and flexibility needs, which are sourced through market-based mechanisms. Article 7bis of the Electricity Law assigns Elia the task of analysing the need for strategic reserves. Elia performs a yearly analysis of the adequacy needs for the Belgian system for the upcoming winter period and provides an outlook for the next two winter periods. Elia also closely collaborates with its European colleagues of ENTSO-E to perform a yearly European adequacy assessment. Article 7bis, §4bis of the Electricity Law states that each biennial period, the TSO shall analyse the adequacy and flexibility needs of the Belgian electricity system for the next ten years.

Strategic reserves are procured following a market-based tendering process amongst the eligible capacity. The system has been approved by the European Commission for a set period, ending in 2022. The strategic reserve operates 'out-of-market', which means that the capacity held as strategic reserve, cannot participate in the energy market like any other capacity. It can only deliver energy when called upon during periods of anticipated electricity shortfall, typically reacting to a strong market signal and/or a signal given by the TSO.

TSOs safeguard the continuity of energy transactions during normal circumstances as well as during an emergency, a black-out or restoration state while applying the System Defence Plan and the Restoration Plan if needed. Market activities and market accompanying processes are only suspended as a last resort.

Alongside the Belgian energy only market, we established a Capacity Remuneration Mechanism (CRM) to be able to deliver capacity from 1 December 2025 onwards. According to Belgian law, the nuclear power stations will be closed by 2025. Therefore, additional capacity will have to be procured in the market. The bidding process for this CRM-auction started in October 2021, accommodating enough time for additional capacity to be contracted. During the drafting of this Plan the Belgian Government received the final approval on the principal of the CRM-auction as well as on its necessity by the European Commission. By the end of November 2021, the Government reassessed the Belgian situation in terms of security of supply and cost of electricity. If this monitoring shows that there is an unexpected security of supply problem, the government will take appropriate measures such as adapting the legal nuclear phase-out calendar for a capacity of up to 2 GW.

Combining a well-functioning energy market (both energy only and whenever necessary a capacity 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.

#### 4.4. Market suspension conditions

Pursuant to article 35 to 39 of the network code on emergency and restoration, the TSO developed a proposal for rules concerning the suspension and restoration of market activities in December 2018. The National Regulatory Authority (NRA) CREG, by means of the CREG-Decision (B)1941 of 19 September 2019, rejected this first proposal. The TSO, Elia, will submit a new proposal by the beginning of 2022.

Although a final proposal has not yet been approved by the NRA, the Restoration Plan, as described in chapter 4.1.11, defines a context of the market suspension conditions. The Restoration Plan defines how market suspension will be notified, and who will be the responsible parties involved.

#### 4.5. Regional and bilateral procedures and measures

Pursuant to the requirements on solidarity and regional cooperation, the Pentilateral Energy Forum established a Memorandum of Understanding on risk preparedness in the electricity sector, which can be found in annex 1 of this plan. It provides an overview of the work that will be done concerning the establishment of possible common measures.

The common measures that will be assessed within the Penta context will build upon existing inter-TSO agreements, as well as other relevant solidarity mechanisms. An example of this is the EU civil protection mechanism. More specifically, the following measures will be analysed in more detail: cross-border usage of reserve capacities and flexible loads, exchange about demand disconnection plans, surveillance of the short-term security of electricity supply, coordinated information regarding saving appeals to the public, support with electric equipment, knowledge and expertise, and usage of mobile generators. Within the context of Steering Group II of the Pentilateral Energy Forum these measures will be further analysed based on their technical, financial and legal possibility. While this last version of the Risk Preparedness Plan was being drafted the different Penta members already had a chance to share a first national analysis of these proposed measures.

## 5. Stakeholder consultations

### 5.1. Consultation of stakeholders

To ensure a wide support, stakeholders were involved during the various stages of drafting the Risk Preparedness Plan. In this context, a Risk Preparedness Stakeholder Task Force was created, composed of representatives of the following public and private partners:

- The Directorate General for Energy;
- The National Crisis Centre (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 Defence of Consumer Interests.

As such, the composition of the Risk Preparedness Stakeholder Task Force goes beyond the minimum requirements listed in annex 1 of the Risk Preparedness Regulation.

The Task Force met on three occasions during the elaboration of the draft Risk Preparedness plan 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.

The stakeholders of the Task Force mentioned above were consulted on the overall structure and content of the draft Risk Preparedness Plan through a digital survey. 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.

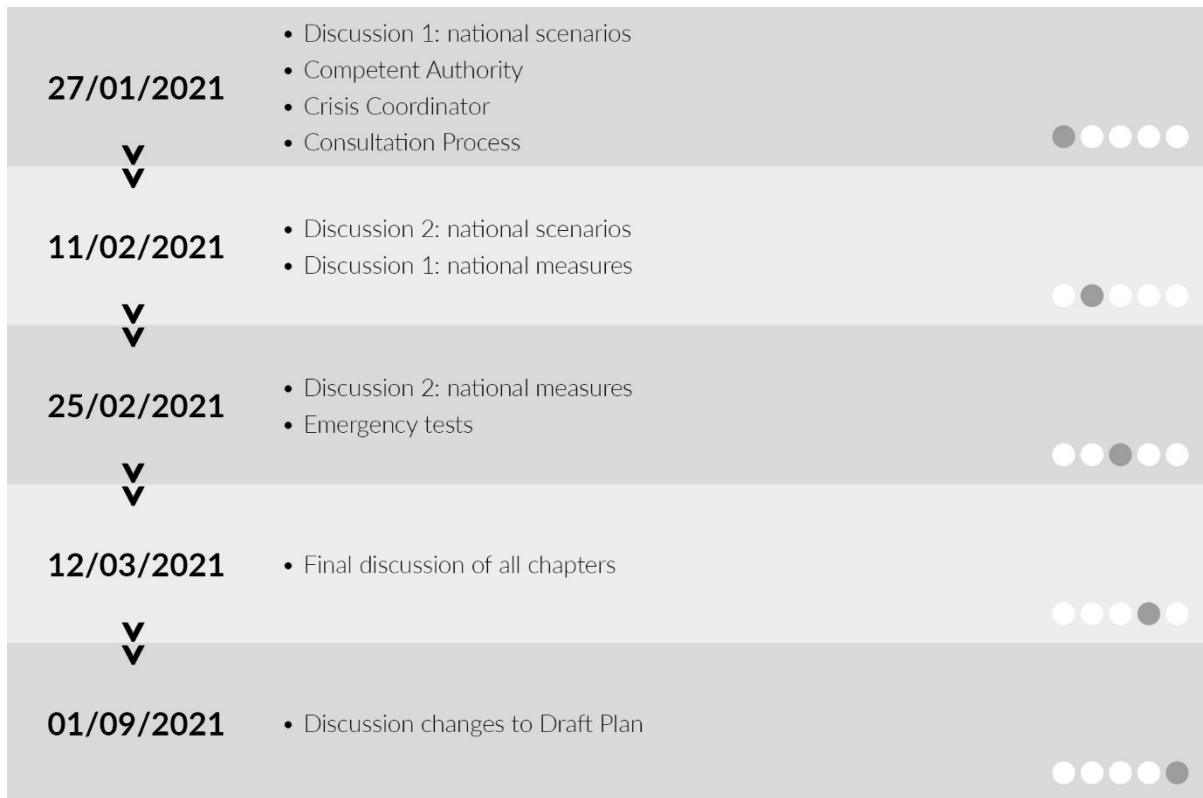
The input that was received on the topics discussed above was used to create the overall structure and goals of the first draft of the Risk Preparedness Plan.

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 Centre (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 to discuss the topics shown in the figure below.

Figure 9: 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.

Prior to the final deadline of the Risk Preparedness Plan, an extra meeting of the Risk Preparedness Drafting Team took place on 1 September 2021. The goal of this extra meeting was to go through the changes that the draft Risk Preparedness Plan had undergone. It was explained to the stakeholders present that the changes were based on recommendations and best practices as shared within the Electricity Coordination Group (ECG) and the Pentalateral Energy Forum.

A final consultation of the stakeholders, as listed above, took place between 18 October and 16 November 2021. Apart from minor grammatical and linguistic comments, the stakeholders informed the DG Energy that they had no further comments on the final Plan. The main reason for this being that they had participated in drafting the Plan from the start in 2020 and that the comments were implemented all through the process. All stakeholders agreed that certain comments will need to be dealt with in the next risk preparedness cycle. This is mentioned throughout this Risk Preparedness Plan. The specific topics that will be taken up in the next couple of years are:

- A more in-depth analysis of the impact and probability of the identified electricity crisis scenarios
- A revision of the national regulatory and legislative framework for electricity crisis management

## 5.2. Consultation of the regional authorities

In parallel with 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 were actively informed during the monthly **CONCERE-ENOVER** meetings<sup>13</sup>. In addition, a topical meeting was organised on 30 November 2020. The CONCERE-ENOVER members were also given the opportunity to give their feedback on the initial proposal of the national electricity 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.

Together with the stakeholders mentioned above, the regional authorities were consulted on the final Risk Preparedness Plan between 18 October and 16 November 2021.

## 5.3. Regional consultation

An essential factor in setting-up an effective and efficient crisis management framework is ensuring its overall consistency. Therefore, the interaction between the regional procedures and measures identified in the previous chapters and the policies set-out at national level should be analysed. Furthermore, the cross-border impact of the measures of individual countries needs to be assessed.

In this context, the Pentalateral Energy Forum organised a regional assessment of the draft national Risk Preparedness plans amongst its Member States. The focus of this assessment was on cross-checking the consistency of the procedures and measures at national, bilateral and regional level. To achieve this, competent authorities shared the English version of their draft Risk Preparedness plans with the Support Group II of the Forum in May 2021. A dedicated meeting of Support Group II of the Forum was then organised in June 2021 to exchange initial concerns and make clarifications. To align this initiative with the activities foreseen within the Electricity Coordination Group, the European Commission was invited to the meeting, and a representative of the Forum was available to give a presentation of the main results of the outcomes of the regional assessment

The outcomes of this meeting were included in the progress report on the implementation measures of the regional aspects of the Risk Preparedness Regulation by the Pentalateral Energy Forum, which were presented to the Directors-General at the end of June 2021. Afterwards, Penta-members had until the mid of July to file written comments to the draft national Risk Preparedness plans. Member States took these comments in account when finalizing their Risk Preparedness plans by 5 January 2022.

---

<sup>13</sup> 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 Foreign Affairs



## 6. Emergency tests

### 6.1. Regional emergency tests

Penta-members carried out a first joint exercise in 2018 based on the MoU on Emergency Planning and Crisis Management concluded in 2017.

The successful exercise enabled the sharing of different national crisis management mechanisms and established contact between crisis management bodies in the Penta region for the first time. The report after the joint exercise expressed the following:

1. “The exercise goals were met:
  - The participants got to know each other better, even in a national setting, and strengthened the Penta network,
  - Awareness was raised on national cross-border issues arising from a Europe-wide scarcity situation,
  - Some best practices were identified and explored,
  - This exercise was a first step in jointly working towards an even better collaboration within the Penta community.
  
2. Penta sets a good example, but needs to keep on running:
  - Penta is a front runner amongst multilateral forums in the area of crisis management and leads the effort on cross border harmonization
  - Penta needs to build a road map for future improvements in effective crisis prevention and management based on the lessons learned and,
  - The effort needs to be expanded to the EU-level
  
3. We have to be aware that, in order to maintain grid stability, the technical solution always prevails over political solutions.
  
4. At TSO level, there are mechanisms and tools in place to coordinate, to operate and to communicate on a daily basis with each other, but in case of electricity crisis prevention and management a formalization of this platform should be encouraged.”

Given the success of the first joint exercise, and the identified action points, the Penta members acknowledge the importance of continuing to regularly organize joint exercises. Pursuant to article 12 of the Risk Preparedness Regulation these will be held biannually starting in the fall of 2022. The exercises will mainly aim to assess the coordination, communication and mutual assistance mechanisms.

While this latest version of the Risk Preparedness Plan was being drafted the specifics of the next joint exercise, which will take place during the fall of 2022, are being discussed within the context of Steering Group II of the Pentilateral Energy Forum.

### 6.2. National emergency tests

The question of organising additional national emergency tests was part of the digital survey sent to the stakeholders and the regions, as discussed in more detail in chapter 6.1. All stakeholders agreed that it will be beneficial to organise national emergency tests alternating the regional emergency tests.

The national emergency tests will build further on the lessons learnt from the national crisis exercise organised in 2016, as well as the separate crisis exercises the different stakeholders organise separately. The national crisis exercise specifically focused on testing the Procedure in the case of an Electricity Shortfall. The exercise was aimed at testing the detection of a possibility of an electricity shortfall. In practical terms this means that the exercise was mostly aimed at testing the first steps of preparation as

described in the common procedure, in chapter 4.1.9.1. 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 the Economy
- 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 NCCN and the Directorate-General for Energy. Every Department, cell and actor involved took it upon themselves to act upon the recommendations following this exercise. In mid-April of the following 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 foundation for the next national crisis exercise in light of the Risk Preparedness Plan.

The stakeholders agree that it will be beneficial to start organising 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 :  
Memorandum of Understanding on Risk Preparedness

# MEMORANDUM OF UNDERSTANDING OF THE PENTALATERAL ENERGY FORUM ON RISK PREPAREDNESS IN THE ELECTRICITY SECTOR

The Ministers for Energy of the Pentalateral Energy Forum, consisting of Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Switzerland, hereinafter referred to as the “signatories”, wish to confirm their intention to maintain and strengthen their existing cooperation on risk preparedness in the electricity sector.

The signatories have regard to Article 15 of Regulation (EU) 2019/941 of the European Parliament and of the Council on risk preparedness in the electricity sector and repealing Directive 2005/89/EC of the European Parliament and of the Council (‘Risk Preparedness Regulation’).

They take note of the legally non-binding Commission Recommendation (EU) 2020/775 of 5 June 2020 on the key elements of the fair compensation and other key elements to be included in the technical, legal and financial arrangements between EU Member States for the application of the assistance mechanism under Article 15 of the Risk Preparedness Regulation.

## Considering:

- existing legal provisions from the Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation, the Commission Regulation (EU) 2017/2195 of 23 November 2017 establishing a guideline on electricity balancing, the Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration, Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity and Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU;
- that the Ministers for Energy of Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Switzerland have signed a memorandum of understanding of the Pentalateral Energy Forum on emergency planning and crisis management for the power sector on 26 June 2017, that these countries have been closely cooperating within the Pentalateral Energy Forum in order to prevent electricity crises, and that they concur to assist each other in case of an electricity crisis, without exclusion, and in a spirit of solidarity and trust as laid down in the Risk Preparedness Regulation;
- that the “market-first” principle should apply in managing crisis situations and that all market-based measures should be given priority to mitigate the effects of a potential supply disruption. Non-market-based measures shall be activated in an electricity crisis only as a last resort if all options provided by the market have been exhausted or where it is evident that market-based measures alone are not sufficient to prevent a further deterioration of the electricity supply situation;
- that a signatory should only request assistance to prevent or manage electricity crises if all national measures in the requesting Penta country’s risk preparedness plan and inter-TSO (Transmission System Operator) support measures have been exhausted or where it is evident that these measures are not sufficient to prevent a further deterioration of the electricity supply situation;

- that security of supply, including risk preparedness in particular, is a national responsibility but national decisions can impact the EU internal electricity market, neighbouring countries and the Pentalateral Region;
- that cross-border and national grid infrastructure is essential for the security of supply in the Pentalateral Region;
- that a better mutual understanding of national concerns (energy mix, resource and transmission adequacy, flexibility needs, peak capacity, emergency plans, risk management plans) and common measures are necessary for efficient crisis mitigation;
- that mid- and long-term adequacy assessments on a national, regional and European level as well as the continuous improvement of their respective methodologies contribute to a better mutual understanding of security of supply and help identifying and mitigating security of supply issues from a regional perspective at an early stage;
- that common measures are helpful to ensure risk preparedness on a national and regional level in an effective and efficient manner;
- that this Memorandum of Understanding replaces the Memorandum of Understanding of 26 June 2017 on emergency planning and crisis management for the power sector;

with the intention to:

- lay down a framework for cooperation in the Pentalateral Region with a view to preventing, preparing for and managing electricity crises in a spirit of solidarity and transparency and fully respecting the requirements of a competitive internal market for electricity and the operational security procedures of the transmission network operators. This should also include simultaneous crisis situations affecting more than one Penta country;
- bring together the relevant representatives from Ministries, Transmission System Operators (TSOs), National Regulatory Authorities (NRAs) and potentially other stakeholders;
- strive for a joint coordination of regional measures to be implemented in case of a crisis situation, including possible implementation of rules for curtailment of interconnection capacities and load shedding, while ensuring compatibility with the internal energy market;
- prepare for the occurrence of a situation which may not be solved with market-based measures or existing operational procedures of the transmission system operators alone and which may require competent authorities to take non-market-based measures;
- refer to the Memorandum of Understanding as part of the national risk preparedness plans of the signatories in accordance with Article 10 of the Risk Preparedness Regulation;

have agreed the following:

#### Definition of an electricity crisis

- All countries share a common understanding that an electricity crisis is constituted by a present or imminent situation in which there is a significant involuntary electricity shortage.
- A regional electricity crisis is an electricity crisis simultaneously affecting more than one country within the region of the Pentalateral Energy Forum at the same time.

#### Confidential common contact list

- All countries will share a confidential common contact list with names and contact details of all entities involved in crisis prevention and management, which contains at least the competent authority, the crisis coordinator, as well as the National Regulatory Authority (NRA) (if involved in crisis situations) and the Transmission System Operators (TSOs) of each country, and which

will be updated annually by the Benelux Secretariat, unless circumstances warrant more frequent updates.

- All countries pledge to keep the others informed of their organisation and the evolution of their organisation.
- When communicating with another Penta country, a communication protocol will be followed. Unless detailed otherwise in this communication protocol, representatives of Ministries, TSOs, NRAs communicate with their respective peers, with the exception of early warnings that should be issued by the relevant Competent Authorities to all contacts of the confidential common contact list.

#### Exchange on security of supply situation and the functioning of crisis management policies

- Experts from the Ministries, NRAs and TSOs of the Pentalateral Region will meet regularly to discuss the security of supply situation on a national and regional level as well as the functioning of national and regional electricity crisis management policies.
- Upon request of one of the signatories, a meeting or call will be organized at short notice.
- If deemed necessary by one of the signatories, an invitation to the meeting can be extended to other entities, provided that all other regular participants accept this.

#### Penta regional scenarios

- Relevant regional electricity crisis scenarios for the Pentalateral Region will be identified by the Pentalateral Energy Forum, included in the national risk preparedness plans and revised every four years, unless circumstances warrant more frequent updates.
- These regional scenarios for the Pentalateral Region should be consistent with and complementary to the national electricity crisis scenarios as identified by the countries of the Pentalateral Energy Forum.

#### Information on an electricity crisis

- In case of an imminent electricity crisis, or when confronted with an electricity crisis, the competent authority of the affected country will inform all competent authorities of the Pentalateral Region of the situation, the measures taken and planned at national level and the possible regional measures identified.
- The competent authority of the country, having faced an electricity crisis, will provide an ex-post evaluation report during a dedicated meeting with experts from Ministries, NRAs and TSOs of the Pentalateral Region. The meeting should result in a list of lessons learnt and may result in an adaptation of the risk preparedness plans.

#### Assistance in case of an electricity crisis

- The signatories intend to, where they have the necessary technical ability, offer each other assistance by means of regional measures. To that end, and with the purpose of protecting public safety and personal security, signatories aim to decide as quickly as possible on regional measures of their choice in order to deliver electricity in a coordinated manner.
- Therefore, the signatories will assess possible measures such as cross-border usage of reserve capacities and flexible loads; exchange about demand disconnection plans; surveillance of the short-term security of electricity supply; coordinate information regarding saving appeals to the public; support with electric equipment, knowledge and expertise; and usage of mobile generators.
- Conditions under which support can be requested and provided should be clear, objective and harmonised. They should build upon and go beyond existing rules and measures for inter-TSO assistance.
- The signatories intend to agree on the necessary technical, legal and financial arrangements for the implementation of the regional measures. Such arrangements should specify, inter alia,

the maximum quantity of electricity to be delivered at regional level, the trigger for any assistance and for suspension of assistance, how the electricity will be delivered, and provisions on fair compensation between the signatories.

- With regard to fair compensation, the signatories will strive for an agreement covering at least:  
(a) the cost of the electricity delivered into the territory of the affected country requesting assistance as well as the associated transmission costs; and  
(b) any other reasonable costs incurred by the country providing assistance, including reimbursement for assistance prepared without effective activation, as well as any costs resulting from judicial proceedings, arbitration proceedings or similar proceedings and settlements.
- In the event of an electricity crisis in which the signatories have not yet decided on regional measures and technical, legal and financial arrangements, they will apply existing measures of cooperation, such as the dedicated Penta standing group on electricity scarcity, or decide on ad hoc measures and arrangements that are most suitable to address the crisis.
- Possible measures of assistance will need to be coordinated with the concerned national TSOs before such assistance is activated.

#### Electricity crisis exercises

- With the involvement of relevant stakeholders, the competent authorities of the signatories intend to periodically test the effectiveness of the procedures developed in risk preparedness plans for preventing electricity crises, and carry out biennial simulations of electricity crises.
- A calendar for the preparation and the execution, as well as a proposal for the format and goals of the upcoming crisis exercises will be presented in Q4 2021.

**This Memorandum of Understanding does not create any rights or obligations under international law and does not intend to replace or modify any existing legal obligations between the signatories.**

**Signed in Brussels on the 1<sup>st</sup> of December of the year two thousand and twenty one.**

**For the Kingdom of Belgium**



**For the Republic of Austria**



**For the French Republic**




**For the Federal Republic of Germany**



**For the Grand Duchy of Luxembourg**



**For the Netherlands**



**For the Swiss Confederation**

