



Luxembourg risk preparedness plan for the electricity sector in accordance with article 10 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

Final version

20 December 2021

Table of Contents

Introduction	3
Competent authority	3
The regional context	3
1 Electricity crisis scenarios	4
1.1 National crisis scenarios	5
1.1.1 Scenario ID 1. Cyberattack on business-critical ICT infrastructure of entities which are physically connected to the power grid	6
1.1.2 Scenario ID 3. Physical attack against critical assets	7
1.1.3 Scenario ID 17. Loss of ICT tools or telecommunication infrastructure required for electric power system operation in or near real-time	7
1.1.4 Scenario ID 24. Large impact industrial or nuclear accident	8
1.1.5 Scenario ID 27. Solar Storm	8
1.1.6 Scenario ID 16. Multiple failures caused by extreme weather situation	8
1.2 Regional crisis scenarios	9
2 Roles and responsibilities	11
2.1 The government and public authorities	12
2.2 System operators	14
3 Procedures and measures in the electricity crisis	14
3.1 National procedures and measures	14
3.1.1 Overview	14
3.1.2 Crisis prevention	15
3.1.3 Crisis management	17
3.1.4 Information	25
3.2 Regional and bilateral cooperation	27
3.2.1 Overview of regional and bilateral cooperation	27
3.2.2 Mechanisms for regional and bilateral cooperation	27
4 Crisis coordinator	32
5 Stakeholder consultations	33
6 Emergency tests	34
A Memorandum of understanding of the Pentilateral Energy Forum on risk preparedness in the electricity sector	36
B Overview of reference documents	42

Introduction

The electricity sector is in a process of change due to the increasing shares of renewable energies and decentralised market players. Meanwhile, power grids in Europe are closely meshed and markets are coupled with one another, which enables significant efficiency gains but also creates dependencies, last but not least for the risk of electricity supply crises. Against this background, the prevention and management of possible crisis scenarios requires efforts on the national as well as on the regional level. Consequently, **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**¹ (hereafter ‘the Regulation’) lays down rules for cooperation between Member States with a view to preventing, preparing for, and managing electricity crises in a spirit of solidarity and transparency and in full regard for the requirements of a competitive internal market for electricity. The Regulation requires EU member states to adopt and publish their risk preparedness plans after a consultation process on national, regional and European level. The present document is Luxembourg’s risk preparedness plan in accordance with article 10, paragraph 8 of the Regulation.

Competent authority

According to the national law on the organisation of the electricity market, the competent authority responsible for the implementation of the Regulation and the preparation of the present plan is the Minister for Energy of the Luxembourg government.²

The regional context

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 to a regional approach. It allows for 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 transmission system operators (TSOs), ministries, regulatory authorities, the European Commission 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 26 June 2007 in Luxembourg.

Security of supply in the electricity sector has always been one of the most important pillars of collaboration within the Pentalateral Energy Forum. To this end, at the beginning of 2020, the Forum received a mandate to work on a well-coordinated regional framework in light of the

¹ Here and in the following, reference documents appear in **bold italic** for better traceability. An overview of all reference documents is provided in Annex B.

² *Loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité*, article 9bis.

Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector (Risk Preparedness Regulation), while at the same time building further on its Memorandum of Understanding (MoU) 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 from all Penta countries within the framework of Support Group II, mainly focusing on security of supply. Competent Authorities and their representatives, as depicted in the table below, actively contributed to the work.

The first two steps that were taken to work on this well-coordinated regional framework was the drafting of a common chapter that was added to the draft Risk Preparedness Plans and that was presented to the Electricity Coordination Group. This was followed by the signing of a new MoU of the Pentalateral Energy Forum on Risk Preparedness in the Electricity Sector on 1 December 2021 in Brussels by the Ministers representing the countries in the Pentalateral Energy Forum. Both documents aim to provide an answer to the requirements as regards regional and bilateral measures pursuant to article 12 and 15 of the Risk Preparedness Regulation. Furthermore, the MoU provides a basis for the work that will be done in the following years on risk preparedness in the Penta Region.

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

Table 1: Competent authorities in the Penta region

1 Electricity crisis scenarios

In Luxembourg's law creating a High Commission for National Protection (hereafter 'HCPN'), a crisis is defined as follows³:

Any event, which, by its nature or effects, is detrimental to the vital interests or essential needs of all or part of the country or the population, which requires urgent decisions and coordination at the national level of the actions of the Government, the administrations, the services and bodies under the authority of the public authorities, and, if necessary, also at the international level.

³ Loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, article 2 (2)

Against the background of this definition, and according to articles 6 and 7 of the Regulation, relevant regional and national electricity crisis scenarios shall be identified as a basis for establishing the risk preparedness plan.

The identification of the relevant electricity crisis scenarios followed the ENTSO-E methodology developed in accordance with article 5 of the Regulation. The methodology considers different classes of hazards being the initiating event for a crisis scenario:

- Natural hazards
- Accidental hazards beyond the (n-1)-security criterion and exceptional contingencies
- Consequential hazards, especially consequences of malicious attacks or fuel shortages

The crisis scenarios derived from these initiating events are ranked according to assessments of the likelihood (based on the expected frequency of occurrence of an initiating event, or a combination of multiple initiating events) and impact considering the indicators expected energy not served (EENS) and loss of load expectation (LOLE). For both indicators, a classification with a five-step scale is used. The combination of the rating with respect to both parameters results in an overall rating of each scenario in a bandwidth between “insignificant” and “disastrous”.

Details of the methodology can be found in the ENTSO-E document ***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.***

1.1 National crisis scenarios

Based on an initial proposal of possible electricity crisis scenarios by ENTSO-E, a detailed analysis identified six national crisis scenarios as particularly relevant with respect to impact and likelihood from a Luxembourgish perspective. As depicted in the following Figure 1, four scenarios have a “Major” rating while two scenarios have a “Minor” rating but are nevertheless included because of their potentially disastrous impact.

It should be noted that the identification of six particularly relevant scenarios does not imply that all other scenarios are irrelevant or even impossible to occur. Indeed, as will be depicted from section 2 onwards, most parts of the present risk preparedness plan apply to any electricity crisis, independent of the specific scenario.

31 crisis scenarios as identified by ENTSO-E

- 1 Cyber attack on entities physically connected to the grid
- 2 Cyber attack on market participants not physically linked
- 3 Physical attack against critical assets
- 4 Physical attack against control centres
- 5 Threatening/blackmailing/hostage-taking of key employees
- 6 Insider attack
- 7 Solar Storm
- 8 Volcanic eruption
- 9 Storm
- 10 Cold Spell
- 11 Heavy precipitation and flooding
- 12 Winter Incident
- 13 Fossil fuel shortage (incl. natural gas)
- 14 Nuclear fuel shortage
- 15 Local technical failure with regional importance
- 16 Multiple failures caused by extreme weather situation
- 17 Loss of ICT for power system operation
- 18 Simultaneous failure of power system primary elements
- 19 Complexity of power system control mechanism
- 20 Unintended violation of N-1 criterion due to human error
- 21 Physical flows don't follow market flows
- 22 Serial equipment failure due to a systematic defect
- 23 Strike, riots, industrial action in power supply chain
- 24 Large impact industrial or nuclear accident
- 25 Unexpected interaction of energy market rules
- 26 Unusually big forecast errors for renewables
- 27 Pandemic
- 28 Heatwave
- 29 Dry period
- 30 Earthquake
- 31 Forest fire

National Assessment

Scenario ID	Impact		Likelihood				
	EENS%	LOLE	Very likely	Likely	Possible	Unlikely	Very unlikely
1	Disastrous	Disastrous	Disastrous	Disastrous	Critical	Major	Minor
2	Disastrous	Critical	Disastrous	Critical	Critical	Major	Minor
3	Critical	Disastrous	Disastrous	Critical	Critical	Major	Minor
4	Disastrous	Major	Disastrous	Critical	Major	Major	Minor
5	Major	Disastrous	Disastrous	Critical	Major	Major	Minor
6	Disastrous	Minor	Disastrous	Critical	Major	Major	Minor
7	Minor	Disastrous	Disastrous	Critical	Major	Major	Minor
8	Disastrous	Insignificant	Disastrous	Critical	Major	Major	Minor
9	Insignificant	Disastrous	Disastrous	Critical	Major	Major	Minor
10	Critical	Critical	Disastrous	Critical	Major	Minor	Minor
11	Critical	Major	Critical	Critical	Major	Minor	Minor
12	Major	Critical	Critical	Critical	Major	Minor	Minor
13	Critical	Minor	Critical	Major	Major	Minor	Minor
14	Minor	Critical	Critical	Major	Major	Minor	Minor
15	Critical	Insignificant	Critical	Major	Major	Minor	Minor
16	Insignificant	Critical	Critical	Major	Major	Minor	Minor
17	Major	Major	Critical	Major	Major	Minor	Minor
18	Critical	Minor	Critical	Major	Major	Minor	Minor
19	Minor	Critical	Critical	Major	Major	Minor	Minor
20	Critical	Insignificant	Critical	Major	Major	Minor	Minor
21	Insignificant	Critical	Critical	Major	Major	Minor	Minor
22	Major	Major	Critical	Major	Major	Minor	Minor
23	Major	Minor	Major	Major	Major	Minor	Insignificant
24	Major	Minor	Major	Major	Major	Minor	Insignificant
25	Minor	Major	Major	Major	Minor	Minor	Insignificant
26	Major	Insignificant	Major	Major	Minor	Minor	Insignificant
27	Insignificant	Major	Major	Major	Minor	Minor	Insignificant
28	Minor	Minor	Major	Minor	Minor	Minor	Insignificant
29	Minor	Insignificant	Major	Minor	Minor	Minor	Insignificant
30	Minor	Insignificant	Major	Minor	Minor	Minor	Insignificant
31	Insignificant	Minor	Major	Minor	Minor	Minor	Insignificant
31	Insignificant	Insignificant	Minor	Minor	Minor	Minor	Insignificant

Figure 1: Luxembourg assessment of national crisis scenarios

The identified national crisis scenarios cover the different classes of hazards that may initiate a crisis, i.e. natural, accidental and consequential hazards and are briefly described hereafter with respect to initiating event(s) and potential impacts. It should be noted, however, that the descriptions are purely illustrative, as neither events nor potential impacts could be precisely predicted and anticipated in all detail.

1.1.1 Scenario ID 1. Cyberattack on business-critical ICT infrastructure of entities which are physically connected to the power grid

Initiating event(s): In this scenario, an intruder would enter one or more critical ICT systems of a TSO, DSO, Luxmetering or of a power plant or major load asset which are physically connected to the power grid. The affected systems would for instance be central SCADA systems, substation SCADA systems, EMS, data storage, or scheduling systems.

Operational impacts: In this scenario, the attacker could for example switch lines or transformers, or manipulate schedules from TSOs towards market partners or other TSOs.

Such an attack may cause unintended outages of lines, transformers, smart meters, power plants etc. with possible overloading on remaining lines and transformers. Switching of lines close to a border or cross-border lines might cause problems in other grids, even though the impact would probably be limited because of the size of Luxembourg.

Security of supply impacts: The possible unintended outages of individual assets and overloading on unaffected lines and transformers may lead to a direct loss of supply. Due to Luxembourg’s import dependency, interconnectors are particularly important and switching all these lines off would result in a blackout. The attack could also cause unintended outages of DSO lines and transformers, or, if targeted at the transformers feeding a particular DSO’s area, could switch off an entire DSO area. The impacts of such an attack may cause loss of supply in certain areas, with an effect in the frequency and load flows in the TSO grid. However, as only Luxembourg is affected, loss of supply will be restrained within limits that do not cause major effects on frequency or load flows in continental Europe.

Energy market impacts: Market partners might not be able to follow schedules or to identify manipulated schedules. The attack might send wrong schedules towards market partners or power plants. The attacker may also be able to deny market access of users.

1.1.2 Scenario ID 3. Physical attack against critical assets

Initiating event(s): Physical attack on critical assets of the electricity supply system, such as power lines, transformers, substations, power plants, or data centres.

Operational impacts: In this scenario, an attacker would destroy technical equipment in the TSO or DSO system. N-1 security could be in danger or no longer fulfilled. Recovery of N-1 security may not be possible in the short term. Grid operators would have to react with congestion management measures, e.g. by switching the remaining elements in order to restore N-1 security (if possible), and/or by activating redispatch and reserves. Loss of grid elements may cause cascading overloads on other elements, possibly also in neighbouring countries. The required maintenance and repair works may imply situations with reduced reliability margins and/or additional planned outages.

Security of supply impacts: The attack may endanger security of supply due to violations of (n-1) security, or even lead to immediate load disconnections. This risk is particularly relevant to Luxembourg at a national level due to its strong import dependency. Potentially destroyed power plants would no longer be able to fulfil their generation schedules and would be missing from the TSOs resource pool to balance the grid. Depending on the time needed to repair assets, loss of supply and emergency measures could remain even for a longer period.

Energy market impact: Market partners are possibly not able to follow schedules or have to reschedule energy trades due to missing connections to other countries or regions. Normal market activities might need to be stopped due to missing grid elements.

1.1.3 Scenario ID 17. Loss of ICT tools or telecommunication infrastructure required for electric power system operation in or near real-time

Initiating event(s): One or more technical failures causing either the loss/unavailability of a substantial part of the telecommunication infrastructure used for the operation of the power system or electricity market, or the loss/unavailability of one or more ICT systems used for the real-time planning and operation of the power system (e.g. grid security calculation, RES generation forecast, measurement system). This could include tools and systems used for energy market operation due to technical failures.

Operational impacts: Initially, the power systems would drift within secure limits of reserves, inertia, voltage stability etc. Remedial measures may need to be invoked at local level, if available, and at regional level if there are insufficient resources locally. As a last resort, these measures can include disconnection of supply or demand assets. If a prolonged incident leads to a sustained deviation from secure operation conditions, this could cause emergency disconnection of generation and demand assets.

Security of supply impacts: Loss of load may be caused through remedial measures implying load or generation assets to be disconnected in a controlled way. If the system runs out of secure operation boundaries due to a loss of control, emergency disconnection may lead to additional loss of load. In a worst-case event, such disconnections can cascade to a blackout situation.

Energy market impacts: Market participants may initially suffer financial losses due to incorrect information or lack of access to some market data. This situation may be aggravated because of

incorrect decisions of the market participants resulting from access to incorrect data. In a worst-case scenario, market suspension could be a last resort measure.

1.1.4 Scenario ID 24. Large impact industrial or nuclear accident

Initiating event(s): A serious industrial accident occurs (e.g. radiation spread from a nuclear power plant, explosion, toxic substance emission from a chemical plant, etc.) due to any reason such as a technical failure, earthquake, sabotage/terrorist attack or human error.

Operational Impacts: Because of unpredictable and unusual electricity production and consumption patterns, it may be hard to balance the power system in such a scenario. Shortages in staff as well as the difficulty of access to control rooms may render the reliable management of the system difficult, and an increased risk of human errors may lead to technical failures and blackouts. In the field, both planned and emergency repairs may be delayed or impossible.

Security of supply impacts: If power plants or control rooms need to be shut down because of the accident, electricity supply may be reduced for a prolonged time. Furthermore, failures resulting from the operational impacts may lead to risks of unsupplied electricity. As a worst-case impact, a partial or total blackout is possible, and may be difficult to recover from, as parts of control area are inaccessible.

Energy market impacts: Energy market operation may be disrupted due to inaccessibility of facilities. Even if possible, market operation will be under highly unusual conditions, with highly unpredictable behaviour, and potentially aggravating the crisis.

1.1.5 Scenario ID 27. Solar Storm

Initiating event(s): The sun sends out a strong Coronal Mass Ejection, e.g. a Carrington-like event. The effects are strongest in the most northern countries of Europe but are also significant in Central Europe.

Operational impacts: Solar storms would lead to an overloading of power system and telecommunication assets and equipment, especially transformers, and thus to a massive blackout at European scale. If not properly secured in advance, primary equipment would suffer long-term damage.

Security of supply impacts: As system operation cannot be continued during a solar storm, supply of electricity would be disrupted at least for the time of the initiating event to pass. Security of supply would be compromised even longer in case equipment suffers long-term damage.

Energy market impacts: There would be the necessity to suspend markets for the duration of the solar storm, as the system would be in blackout state.

1.1.6 Scenario ID 16. Multiple failures caused by extreme weather situation

Initiating event(s): In this scenario, the initiating event would be multiple failures caused by an extreme weather situation – especially extremely high or extremely low temperatures – or an unexpected and (relatively) synchronous failure of multiple grid or telecommunication components of the same type.

Operational, security of supply and energy market impacts: If key elements of the grid were affected, there would be a high risk of cascading failures and unstable system conditions, similar to those described for Scenario ID 3. In case of ITC infrastructure failures (such as wrong

measurements, failing control transmissions, IT equipment failure), impacts would be similar to those described for Scenario ID 17.

1.2 Regional 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 Pentilateral Energy Forum 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 Pan-European perspective⁴. 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 on 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 and/or interdependency among Member States for a large majority of scenarios. Based on ENTSO-E's methodology for deriving a regional rating of crisis scenarios⁵, a Penta-rating of all crisis scenarios was established, as shown in the table below, in which the order is dependent on which scenarios has been rated most often as relevant scenarios in the national and cross-border context.

⁴ENTSO-E report *Risk-Preparedness Regulation – Identification of Regional Electricity Crisis Scenarios*

⁵ 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*.

ID	Electricity crisis scenario	Penta-Rating
1	Cyberattack - entities connected to 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
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 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

Table 2: Penta-rating of ENTSO-E's 31 crisis scenarios

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. 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.

Notably, significant cross-border dependencies arise from the fact that Penta is characterized by high levels of integration and interconnectivity⁶, 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

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

time, integration and interconnectivity also allow to manage risks through appropriate measures.

During the assessment, experts also considered a more generic description of crisis scenarios, by using topical groupings, as a meaningful approach for risk preparedness. 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 – both falling into the category of extreme weather conditions – 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-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.

Electricity crisis scenario – Topical grouping	Penta-Rating
Cyber-attack (ID 1,2)	27.6
Extreme weather (ID 7,9,10,11,12,16,28,29)	22.2
Physical attack (ID 3,4,5,6)	21.9
Technical failure (ID 15,17,18,22)	16.6
Other (ID 19,24,26)	15.4
Fuel shortage (ID 13,14)	11.4
Market rules (ID 21,25)	11.4
Human-related (ID 20,23)	11.0
Natural disaster (ID 8,27,30,31)	9.2

Table 3: Penta-rating of crisis scenarios according to their topical grouping

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 the triggers, the possible chain of events, and the impact those three scenario groupings would have on the electricity supply situation. While cyberattacks 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 Roles and responsibilities

In Luxembourg, the most important bodies involved in electricity crisis management can be depicted in two groups:

- a. Members of the Luxembourgish **government**, especially the Prime Minister and the Minister for Energy, as well as **public authorities**, in particular the High Commission for National Protection (HCPN) lead by the High Commissioner, the Government Commissioner for

Energy, the corps grand-ducal d'incendie et de secours (CGDIS), the police grand-ducale, and the government's information and press service (SIP).

- b. **System operators**, in particular Creos Luxembourg S.A. (hereafter 'Creos') who is the transmission system operator (TSO) and the largest distribution system operator (DSO) in Luxembourg. Besides Creos, there are four other electricity DSOs⁷ and one industrial system operator⁸.

The above bodies are all involved in all phases of crisis management with distinguished roles and responsibilities. An overview is provided hereafter while the detailed procedures and measures are described in section 3.

2.1 The government and public authorities

The **government** is the decision-making entity in case of an electricity crisis. Several government members are involved explicitly in crisis management.

In its role as the competent authority in the sense of the Regulation, the **Minister for Energy** is responsible for the identification of relevant national electricity crisis scenarios (article 6), the establishment of the risk preparedness plan as well as its consultation and publication (article 10-12), the issuing of early warnings and declarations of an electricity crisis to the European Commission and the Member States in the region (article 14), and the ex-post evaluation of an electricity crisis (article 17).

In terms of operational crisis management, the highest decision-making power lies with the **Prime Minister** as depicted in the Government's crisis emergency response plans (see section 3 below).

The most important **public authorities** having distinguished roles and responsibilities in electricity crisis management are the following:

High Commission for National Protection (HCPN)

At the national level, the missions of the HCPN can be divided into four groups:

- coordinating counter-terrorism measures,
- preventing and managing crises of any kind affecting the vital interests or essential needs of all or part of the country or population,
- protecting critical national and European infrastructures,
- contributing to the definition and implementation of the national cyber-security strategy.

At international level, the HCPN represents the country at European Union fora, NATO, Benelux, and any other international organisation dealing with the management of crises and civilian emergency response plans. With Luxembourg's neighbours, it is responsible for establishing and maintaining contact with the organisations in neighbouring countries that have similar or identical responsibilities to those of the HCPN.

The head of the HCPN, the High Commissioner, acts as a link between government, private organisations and the public in any kind of crisis.

⁷ Ville de Diekirch, Hoffmann Frères Energie et Bois s.à.r.l., Ville d'Ettelbruck, Sudstrom S.à.r.l. & Co s.e.c.s.

⁸ Sotel Réseau et Cie S.e.c.s.

Government commissioner for energy

According to the law on the organisation of the electricity market, the Government Commissioner for Energy is responsible, amongst other tasks, for the monitoring of the national energy supply situation.

Corps grand-ducal d'incendie et de secours (CGDIS)

The CGDIS is responsible for civil protection with the following main missions:

- assistance for people who are in need due to accidents, disasters, fire or other damaging events,
- fire prevention and protection,
- combating pollution from radioactive, nuclear, biological or chemical substances,
- protecting property in the event of fire, disaster or other damaging events,
- international assistance in the event of disasters outside the Grand Duchy, and
- ensuring medical emergency services.

Depending on the type and scale of the crisis, CGDIS may be supported by other national services such as the national armed forces, national road administration, etc.

Police grand-ducale

The police are a national service responsible for ensuring internal security. It ensures respect for and contributes to the protection of individual rights and freedoms and acts through preventive, proactive, dissuasive, and repressive actions.

In carrying out their administrative police duties, the Police ensure

- maintaining public order,
- the execution and respect of general and municipal police laws and regulations,
- the prevention of offenses, and
- protection of people and property.

Further tasks result from their judicial police duties. In addition, and pursuant to article 42 of the law on the police grand-ducal, the national armed forces intervene to assist the Police in their missions upon requisition by the competent authorities in the cases provided for by the law.

Information and press service (SIP)

The SIP is the body responsible for circulating communications from the Luxembourg Government. It is attached to the Ministry of State and is under the direct authority of the Prime Minister. The main missions of the SIP are as follows:

- ensuring the communication of information about State activities to the press, the media, the public and interested parties,
- defining and implementing the Government's communication policy with regard to Internet and the social media,
- keeping the Government informed of current affairs dealt with in the press and the media,

- publishing and circulating documents and information of all kinds,
- defining and implementing a policy of promoting open data and access to information, and
- facilitating the work of journalists and media representatives.

2.2 System operators

Based on the European and national legal framework, and specifically pursuant to article 9 of the national law on the organisation of the electricity market, the transmission, distribution and industrial system operators have far-reaching responsibilities for security of supply and the reliability of the electricity system. They are responsible for the planning, execution, maintenance and operation of high, medium and low voltage power grids, and obliged, jointly with producers and suppliers, to guarantee the security of supply of electricity to end customers within the economically justifiable limits.

3 Procedures and measures in the electricity crisis

3.1 National procedures and measures

3.1.1 Overview

Risk preparedness can be structured along different dimensions. For this plan, the following distinction is drawn:

- **Crisis prevention**, prior to the specific knowledge of any concrete incident that might cause an electricity crisis
- **Crisis management**, including both the preparation for an imminent crisis as well as the mitigation of adverse effects during and shortly after the crisis
- **Information**, a horizontal element in parallel to the two aforementioned phases

An overview of the most relevant national procedures and measures is provided in **Error! Reference source not found.** below. Following the structure of the three dimensions depicted above, they are discussed in more detail in sections 3.1.2 - 3.1.4.

It should be noted that neither the overview nor the explanations in sections 3.1.2 - 3.1.4 are meant to be fully exhaustive as further procedures and measures may be applied depending on the specific situation.

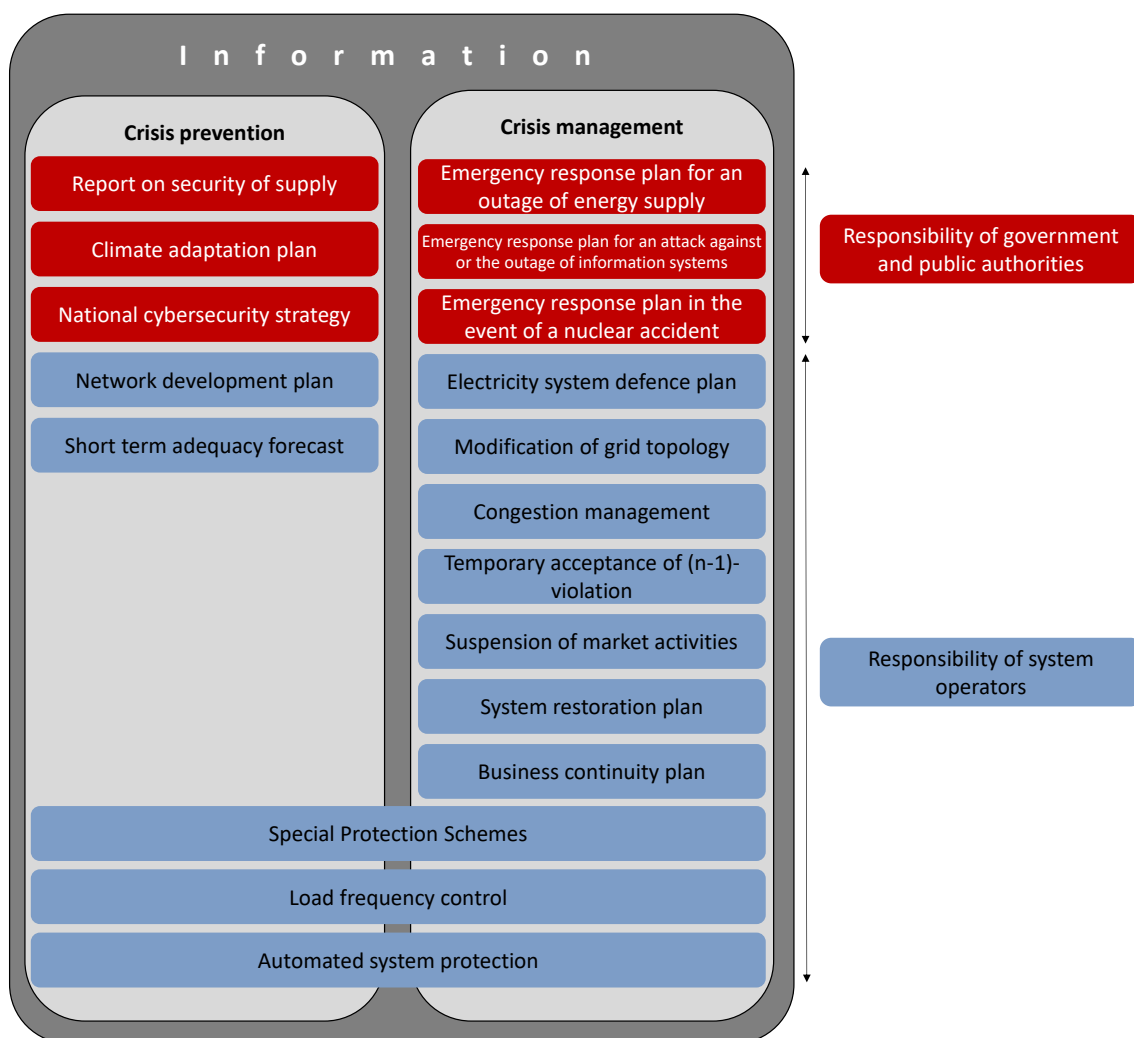


Figure 2: Overview of the most relevant national procedures and measures. Note that original titles for several items are in French. Details are provided in sections 3.1.2 - 3.1.4.

3.1.2 Crisis prevention

One of the main objectives of risk preparedness is to avoid crisis situations upfront as far as possible. Thus, preventive procedures and measures aim to identify potential electricity crisis scenarios and to activate measures early enough to either prevent the initiating event and/or to completely mitigate its negative impact(s) within regular system operations.

3.1.2.1 Preventive procedures and measures by the government and public authorities

Pursuant to article 11 of the law on the organisation of the electricity market, the **Report on Security of Supply**⁹ provides an analysis of the current situation of supply related to generation and demand, the amount of import capacities and the condition of the grid. Furthermore, it introduces an outlook on the expected development concerning the level of security of supply over the following years. The report is updated every two years and builds upon detailed information from the entire electricity sector. Specifically, system operators submit their

⁹ Original title *Bericht über die Versorgungssicherheit im Strombereich in Luxemburg*

inventory as well as their planning for investments in the subsequent decade, allowing for a detailed analysis of Luxembourg's grid infrastructure.

The Luxembourg Government's ***Strategy and action plan for the adaptation to the effects of climate change in Luxembourg (2018-2023)***¹⁰ identifies the impacts of climate change on a broad range of sectors, and presents a list of measures to adapt accordingly. For the case of energy, the document refers to the following three elements:

- Increased impacts of extreme events → Check and adapt existing energy infrastructure for vulnerability to extreme events
- Change in electricity demand → Take measures to raise awareness of energy conservation and deployment of decentralised solar energy and other unused energy sources
- Higher biomass production → Develop biomass plants taking into account sustainability aspects

The ***National Cybersecurity Strategy***¹¹ for the period up to 2025 sets out the guidelines underlying the projects that the Government intends to implement in order to secure cyberspace at all levels. It aims to enable all actors to participate fully in a digital society and to access the new technologies in a secure environment. The measures that will be implemented are designed in the first place to ensure that Internet users are aware and to strengthen their trust in the digital world. Furthermore, they consist in consolidating and strengthening the security and resilience of digital networks and infrastructures. Lastly, the strategy seeks to take account of cybersecurity as a factor of economic attractiveness and to complement the strategy of dynamisation that characterises the digital sector towards the continued development of a high-performance digital economy.

3.1.2.2 Preventive procedures and measures by system operators

The main preventive measure of system operators is to ensure a fully functional, adequate and resilient supply system. Pursuant to article 9 of the law on the organisation of the electricity markets, system operators are, jointly with producers and suppliers, obliged to ensure the security and quality of supply, both in the short as well as in the long-term.

For the long-term, and in accordance with ***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***, they elaborate ***Network Development Plans*** at least every two years. The plans shall contain efficient measures aiming to guarantee the adequacy of their respective system and its security of supply. The network development plan of TSO Creos plays a particularly important role to ensure security of supply in the long-term.

For the short-term, a large number of technical measures are activated automatically as they are embedded in real-time grid-operation procedures and therefore contribute to prevent an electricity crisis. Regular modification of the grid topology and the application of congestion management procedures in the capacity calculation region pursuant to ***Commission regulation (EU) 2015/1222 of 24 July 2015 establishing a guideline on capacity allocation and congestion management*** are standard procedures to control the grid load. In addition, the European legal framework defines further grid related procedures in particular in ***Commission regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system***

¹⁰ Original title *Stratégie d'adaptation aux effets du changement climatique pour le Grand-Duché de Luxembourg*

¹¹ Original title *Stratégie nationale de cybersécurité IV (2021-2025)*

operation (hereafter ‘System Operation Guideline’), which includes amongst others the following operational measures:

- **Load frequency control** serves to compensate imbalances between generation and consumptions and deviations from nominal frequency involved. With respect to the national crisis scenarios, there are various incidents that might cause relevant imbalances. These include attacks against critical assets, industrial accidents or the disconnection of consumers or generation units. The load-frequency control mechanism for the Creos transmission grid is embedded in the common Creos-Amprion load-frequency control area (which is operated by Amprion) of the load-frequency control block of Germany, Luxembourg and Denmark (West).
- **Automated system protection** is part of the real-time grid operation. In the Luxembourgish system such protection procedures exist for the automatic disconnection of demand as a last resort in case of underfrequency configured by Creos in accordance with the requirements of ENTSO-E and are installed for preventing a voltage collapse by blocking the automatic step changing on the high voltage transformers.
- **Special Protection Schemes (SPS)** are case specific measures for unexpected events that emerge and develop in such a short period of time that manual intervention is not possible. SPS are automatically activated when a predefined condition is reached. In the Luxembourgish system a SPS is established for the condition that the connection to the Amprion grid is interrupted. In this case the Creos network will be automatically split to avoid a total blackout in Luxembourg.

The process of **short-term adequacy forecasts** represents a complementary preventive measure. This forecast comprises a regional check and update of short-term active power adequacy diagnosis for shorter timeframes than seasonal outlooks such as the one prepared half-yearly by ENTSO-E. The short-term adequacy forecast perform an analysis of detailed information on production, consumption and available grid capacities. It is executed by the TSO or the Regional Security Coordinator (RSC), respectively.

3.1.3 Crisis management

Crisis management is to be triggered as soon as a crisis becomes imminent and where it cannot be ensured that standard and preventive measures will indeed impede a crisis, and lasts until the emergency situation is overcome. Throughout the phase of crisis management, all appropriate procedures and measures are activated to contain and control the development of the situation as far as possible and to minimise the impact on all affected sectors. This may require certain measures to be maintained although the actual emergency situation has been overcome.

In order to mitigate electricity crises efficiently, specific incidents may trigger different sets of measures that will be applied either separately or complementary to each other, depending on the crisis scenario.

3.1.3.1 Crisis management by the government and public authorities

The **Emergency response plan for an outage of energy supply**¹² represents the Government’s plan for emergency intervention in case of an electricity crisis that may be caused by any of the

¹² Original title *Plan d’intervention d’urgence (PIU) “Rupture d’énergie”*

national crisis scenarios depicted in section 1 or any other scenario affecting security of supply. It determines the required bodies for the crisis management, the definition of emergency measures and procedures for their activation, as well as procedures of information flows among authorities as well as with the public.

Besides the emergency response plan for an outage of energy supply there are eleven such emergency response plans in total, which are regularly reviewed and updated¹³. For the scenarios “nuclear accident” and “cyberattack” that were identified as particularly relevant for Luxembourg (cf section 1), specific response plans are in place, i.e. ***Emergency response plan in the event of a nuclear accident***¹⁴ and ***Emergency response plan for an attack against or the outage of information systems***¹⁵, respectively. Other emergency response plans may affect the electricity sector and involve actors from the sector, irrespective of the question whether the corresponding scenario has been identified as particularly relevant for the context of risk preparedness in the electricity sector in Luxembourg for the sake of this present plan (cf Figure 1). For instance, for the case of flooding, dedicated risk management and emergency response plans exist that include several elements related to energy and electricity in particular¹⁶.

In order to be able to deal with the fact that crisis situations may unfold from different angles and fall into the field of more than one emergency response plan, the same general approach and structure is applied to all of them. This allows complementing coherently certain measures or crisis bodies by elements of adjacent emergency response plans (for instance, in case of an electricity supply shortage caused by a cyber-attack). While the structure deliberately foresees a certain level of flexibility in order to be able to respond to the situation-specific needs and requirements, it is nevertheless to be expected that the emergency response plan for an outage of energy supply is the pivotal element in case of a large-scale electricity outage. The main elements of this plan are as follows:

- In order to evaluate the extent, origin and likely duration of the outage of energy supply, the situation is continuously assessed by the **cell for the evaluation of the risk of an outage of energy supply**. The cell is responsible for following the evolution of the situation and for informing the **crisis cell** about its assessment. It is composed, amongst others, of experts from the High Commission for National Protection (HCPN) and the Ministry of Energy, and is chaired by a representative of Creos.
- The **crisis cell** is activated by the Prime Minister and Minister of State in case of an imminent or present crisis. The cell is responsible for directing, coordinating and monitoring all measures for managing the crisis with the aim to restore normal conditions. Members of the crisis cell are representatives of the relevant ministries, administrations and services depending on the nature and scope of the crisis. The crisis cell can be expanded depending on the circumstances for instance by representatives of the energy sector or representatives of other relevant ministerial departments.

¹³ The eleven emergency response plans are Nuclear Emergency; Extreme Weather Conditions; Chemical, biological, radiological or nuclear substances; Terrorism; Influenza and pandemics; Flooding; Power Cut; Ebola; Drinking water; Cyber; and Mass casualties.

¹⁴ Original title *Plan d'intervention d'urgence (PIU) en cas d'urgence nucléaire*

¹⁵ Original title *Plan d'intervention d'urgence (PIU) "Cyber"*

¹⁶ Cf *Hochwasserrisikomanagementplan-2021-2027*

- The crisis cell can authorise an **operational cell** to implement, execute and supervise the directed measures and actions. An operational cell is chaired by a person appointed by the leader of the crisis cell.
- The task of the **cell for communication and information** is to inform the population and the media about the crisis situation.

Legally, temporary measures ordered by the government in an imminent or present crisis situation aiming to safeguard the electricity supply are covered by article 13 of the law on the organisation of the electricity market. It should be noted that such measures do not give rise to any form of financial or other type of compensation, and do not require the prior agreement of the electricity consumers concerned.

Specifically, measures may be activated by the crisis cell in order to minimise the overall impact on national economy and social life, such as

- the activation of the national demand disconnection procedure as depicted in the system defence plan (see section 3.1.3.2 below) by system operators
- the activation of the restoration plan (in case of a blackout situation) by system operators
- removal of physical impact (e.g. overthrown trees in overhead lines), emergency repair of transmission infrastructure, and installation of mobile generators by CGDIS and system operators
- calls to temporarily lower consumption on a voluntary basis

Meanwhile, system operations and other bodies do not necessarily have to wait for instructions from the Government in case of a crisis, as they often have dispositive power to activate a large number of measures themselves, as laid out in the various plans governing their roles and responsibilities. Indeed, necessary response times for operational measures are often extremely, such that related decisions need and can be taken by system operators without prior approval. A concrete example are load shedding plans described that do not require the authorities' approval before activation (for details, see section 3.1.3.2 below).

Crisis management in case of a cyberattack

In the specific case that the crisis is the result of a cyberattack, and depending on the role of respectively for energy therein, crisis management either follows or is complemented by the steps described in the ***Emergency response plan for an attack against or the outage of information systems***. Drawn up using the same logic as the ***Emergency response plan for an outage of energy supply***, the plan foresees the following bodies:

- The **crisis cell** is activated by the Prime Minister and Minister of State in case of an imminent or present crisis. The cell is responsible for directing, coordinating and monitoring all measures for managing the crisis with the aim to restore normal conditions. Members of the crisis cell are representatives of the relevant ministries, administrations and services depending on the nature and scope of the crisis. Depending on the circumstances, the crisis cell may be expanded by including representatives of further relevant ministerial departments and supplemented by representatives of Internet Service Providers and further organisations that are affected by the attack.
- The crisis cell can authorise an **operational cell** to implement, execute and supervise the directed measures and actions. It is chaired by a person appointed by the leader of the crisis cell.

- The role of the **cyber risk assessment cell** is to monitor the situation and to inform the crisis cell about its assessment.
- The task of the **cell for communication and information** is to inform the population and the media about the crisis situation.

In the case of an electricity crisis caused by the cyberattack, mitigating measures emanating from the Emergency response plan for an attack against or the outage of information systems may be activated. The crisis cell assesses the degree of urgency and the impact of the incident on Luxembourgish territory in order to determine the severity of the situation and to identify all systems impacted directly or indirectly (collateral damage). Based on the results of this assessment, the coordination and cooperation between the actors involved as well as the international cyber emergency response team (CERT) community can be organised. The role of the cyber risk assessment unit role is to monitor any critical national cyber-security incident or threat and to continuously keep the crisis cell informed. It consists of experts and offers a strengthened surveillance and vulnerability analysis within the national emergency response plan. It identifies potential targets, listed according to the type of attack, and ensures an upgrading and protection of threatened information systems. The unit can implement protective measures where targets have been confirmed and preventive measures where potential targets have been determined. It can also partially or totally isolate a target by disconnection if deemed necessary and appropriate.

If the event constitutes a crisis of significant magnitude and considerable impact, the crisis cell can request support by public administration experts in the field of information and communication system security through the activation of the national cyber reserve. For specific areas, the reserve can be supplemented by experts from the private sector or from international organisations of which Luxembourg is a member.

Further assistance can be requested via non-governmental CERTs.¹⁷

Crisis management in case of a nuclear accident

For the crisis scenario of a nuclear accident, the preparatory measures according to the ***Emergency response plan in the event of a nuclear accident*** are applied.

- The Prime Minister activates the **crisis cell**. The crisis cell initiates, coordinates and monitors the execution of all the measures intended to deal with the crisis and its effects. In addition, the crisis cell works closely with its foreign counterparts.
- The main task of the **radiological evaluation cell** is to suggest appropriate emergency measures to the crisis cell, monitoring changes to the state of the damaged reactor, the scale and changes to radioactivity in the environment and its impact on the population. The aim is to provide the best possible protection for the population against all the dangers associated with ionising radiation. The members of this cell also work closely with their foreign counterparts. The radiological evaluation cell comprises experts from the Department for Radiation Protection at the National Health Directorate and members of CGDIS.
- The task of the **communication/information cell** is to support the crisis cell in its efforts to coordinate communication between the authorities and the population. It keeps the media

¹⁷ The cyber emergency response community Luxembourg initiative “cert.lu” serves to enhance the collaboration between public and private CERTs in Luxembourg.

and citizens informed of the changing situation as well as the prescribed preventive and protective measures.

As soon as the Luxembourg 112 emergency call centre is informed of a nuclear accident, it alerts the radiological evaluation cell, which immediately carries out an evaluation of the information available. If the accident is likely to pose a danger to the population, the High Commissioner for National Protection is informed.

After consulting with CGDIS and the Department for Radiation Protection at the National Health Directorate (Division de la radioprotection de la Direction de la santé), the High Commissioner for National Protection informs the Prime Minister and Minister of State who decides whether to activate the crisis cell.

The execution of this plan falls within the competency of the Prime Minister and Minister of State, the Minister for Home Affairs and the Minister for Health. All further ministries, agencies and departments of the State are bound to cooperate with the implementation of the plan using all the means available to them. Local authorities are considered key partners in this process.

For the crisis scenario of a nuclear accident, mitigation measures according to the **Emergency response plan in the event of a nuclear accident** are taken. These measures (taking shelter, taking potassium iodide tablets, evacuation) mainly serve to protect public health but may corrupt the ability to control the energy supply system. In case that power plants or control centres are within the region of contamination, the operation of the electricity system will be adapted to the emergency situation in order to maintain the electricity supply as far as possible. With respect to the Luxembourgish transmission grid, this is achieved by transferring the functionalities of the main control system to backup systems that can be operated in a decentralised way.

In case the event leads to a shutdown of major power plants in the region of Luxembourg and its surroundings or if grid operation is significantly disturbed, cross-border support from energy suppliers and system operators of less affected regions may be needed in order to maintain the electricity supply.

3.1.3.2 Crisis management by system operators

In case of an imminent or present crisis, a variety of measures is available to system operators to limit its impact or to avoid it altogether. The order for activating these measures depends on the type of crisis scenario and the expected effectiveness.

Several corrective measures in real-time may be executed by system operators to relieve highly loaded lines and transformers. While these measures are part of daily system operation to ensure system security, they are also crucial for the case of specific crisis scenarios.

- The unavailability of transmission lines or generation units, for instance caused by a physical or cyberattack, severe accidents or extreme weather situations may cause overloads of the transmission and distribution grids. **Modification of the grid topology**, e.g. by changing the interconnection of lines in substations and/or coupling or decoupling of busbars, is a measure that can be taken rapidly and mostly remotely with the aim to avoid unacceptable loadings of assets that may cause further outages.
- Topological measures may be supplemented by applying **congestion management** in a grid convenient way, such as redispatch of power production from one location to another. Due to the small size and the properties of the national energy supply system, congestion management potential in Luxembourg is very limited.

- The system operator may also accept a **temporary violation of the (n-1) security** criterion provided that this allows to avoid the activation of measures with extensive impact on clients and market participants (disconnection of generators/consumers, restriction or suspension of the energy market) and to regain (n-1) security after short time. Such temporary non-compliance with the (n-1) security criterion is compatible with the article 35 of the System Operation Guideline.

In situations where the above corrective measures in real-time have not been effective to safeguard security of supply, system operators are equipped with more exceptional measures and procedures for crisis management. Besides national law governing roles and responsibilities for system security, the **System Operation Guideline** as well as **Commission Regulation EU 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration** (hereafter '**Network Code E&R**') provide a European framework with harmonised rules for technical and organisational measures to prevent the spread or amplification of an incident in a national network and the spread of disturbances or blackout conditions to other networks

- In line with article 24 of the **System Operation Guideline**, TSO Creos has developed and adopted an internal **Business Continuity Plan** detailing its planned responses in a crisis situation. Critical business processes have been identified, and mitigation procedures are defined to mitigate the negative impacts by means of measures in the field of IT, telecommunication, critical infrastructure, etc. The plan is an important element to avoid business interruption or at least reduce downtimes to a minimum in case of an emergency. The plan is reviewed and tested regularly to confirm or adjust critical processes, and to train and verify the technical solutions and organisational recovery procedures.
- In a similar vein, several parts of the energy sector are declared as critical infrastructures. National law¹⁸ requires owners or operators of those infrastructures to develop **Business Continuity Plans** which shall include at least the following:
 - characteristics of the critical infrastructure;
 - risk identification, analysis and assessment ;
 - risk reduction measures and preventive strategies;
 - business continuity measures.
- **Demand disconnection** is a tool that can be used as a last resort by the system operators of to prevent the emergence of major incidents and to limit their consequences when they occur. The **System Defence Plan**, collaboratively drawn up by Luxembourg's electricity system operators, defines the circumstances and conditions under which demand disconnection may be used by electricity system operators, the responsibilities and decision-making procedures associated with the practice of demand disconnection, its operational modalities, as well as the priority rules for demand disconnection of customers with the least damage. It is designed for the current structure of Luxembourg's electricity grids, but also to be easily adaptable to potential changes, in particular possible developments in interconnections with neighbouring grids or in the deployment of control-command systems that facilitate the implementation of demand disconnection.

¹⁸ *Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection*, article 5 ; *Loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale*, article 8

Demand disconnection is used to ensure operational security of the transmission grid (based on the safety analysis, and in addition to the available corrective measures) or in case the grid is in an emergency state and no corrective measures are available to restore the normal state. An emergency state of the grid may occur in case of significant frequency deviations or malfunctions of tools, equipment, and installations.

The process of automatic and manual demand disconnection is described in sections 3.1.1 and 3.2.5 of the electricity system defence plan. As there are no large power plants connected to the Creos transmission grid, and the installed capacity of renewable energy sources like wind, photovoltaics and biomass is still rather small¹⁹, the potential for shedding generation is highly limited and therefore not particularly relevant in the context of possible measures for national crisis scenarios.

Section 2.2. (“situations and feared events”) of the system defence plan introduces the circumstances to initiate manual load shedding, while section 3.2.5 (“manual demand disconnection procedure”) introduces the coordination processes between the system operators, the operational procedures, priority rules and disconnectable consumer groups in hierarchical order. The main provisions are briefly summarised in the following paragraphs.

The activation of demand disconnection can be caused by an electricity shortage observed or anticipated by the system operator, in particular a significant imbalance between electricity supply and demand, the limitation of import capacities below an adequate level to ensure supply in Luxembourg or grid failures resulting in extensive overloading. The measure aims at preventing a cascade of overloads and a collapse of voltage or frequency, which would likely result in a total collapse of the grids in Luxembourg.

The disconnection follows a predefined priority ranking regarding the urgency of electricity supply. This hierarchy is set up in order to meet the country’s essential needs and to limit the consequences of demand disconnection as much as possible.

The priority list of electricity consumers comprises the following three levels of priority (cf. section 3.2.5.5 of the aforementioned plan):

- Level 1: strategic national defence facilities and vital communication centres, hospitals, railways, airports, residential consumers, and non-industrial professional consumers with a peak demand of max. 1 MW.
- Level 2: industrial sites classified in accordance with the European SEVESO directive.²⁰
- Level 3: consumption sites in the service and public sectors with a peak demand greater than 1 MW, industrial sites not falling under the European SEVESO directive, and certain previously defined consumer groups (e.g. electric heating systems and private charging stations).

Consumers with the lowest priority level (i.e. level 3) are disconnected first, while consumers belonging to the highest priority level are disconnected last.

¹⁹ Automatic disconnection capabilities for specific situations are usually integrated in those units.

²⁰ *Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC*

In case of an enduring crisis situation, the disconnection scheme may apply a rotational procedure consisting in alternately disconnecting different groups of consumers within the same level for a limited period of time.

Due to the country's strong dependence on imports from neighbouring countries any action to avoid imbalance between generation and demand in Luxembourg, and in particular demand disconnection, must be established in accordance with the measures taken by the German TSO Amprion, and if necessary, by the Belgian TSO Elia as well as the French TSO RTE.

- In accordance with the **Network Code E&R**, Creos has drawn up **Rules for Market Suspension and Restoration**. As Luxembourg is in a common electricity with Germany, it does not have separate rules for the suspension and restoration of market activities, but follows the rules established for the common DE/LU market, including non-discriminatory principles of imbalance settlement for Luxembourg grid users in line with the imbalance settlement rules applied in the context of market suspension in Germany.

As a general rule, market activities can only be suspended if other safeguard measures are no longer available. The market suspension rules are therefore limited to emergency situations and subject to strict conditions as proposed by German TSOs and approved by the German Regulator Bundesnetzagentur²¹.

It should be noted that

- the activities of the DE/LU common market will not be suspended by Creos but by the German TSOs, and that
- an interruption of supply in the Creos system is not a sufficient precondition to justify a suspension of the DE/LU common market activities by the German TSOs.

After a blackout, the TSOs are responsible for ensuring that the network is restored and that market activities are re-established as quickly as possible. A restoration of market activities can only take place if the incidents at the origin of the suspension are resolved and once the concerned market players have been informed by the TSOs.

The rules furthermore stipulate that Creos sends all relevant notifications and information concerning the suspension and re-establishment of the DE/LU common market activities to the relevant Luxembourg entities as soon as possible and after consultation with the German TSOs.

- In case that the remedial measures have not been successful and the system falls into a partial or total blackout condition, a structured restoration of energy supply according to the **System Restoration Plan** is initiated.

Since there are currently no large power plants connected to the Creos transmission grid, Creos is not capable to restore the Luxembourgish energy supply on its own. However, the Vianden pumped storage plant (located in Luxembourg but connected directly to the German Amprion grid) plays an important role for grid restoration in the region, including Luxembourg.

²¹ *Bestimmungen für die Aussetzung und Wiederaufnahme von Marktaktivitäten und die Bestimmungen für die Abrechnung im Falle einer Aussetzung von Marktaktivitäten gemäß Artikel 36 Abs. 1 und Artikel 39 Abs. 1 i.V.m. Artikel 4 Abs. 2 e und f der Verordnung (EU) 2017/2196 der Kommission vom 24. November 2017 zur Festlegung eines Netzkodex über den Notzustand und den Netzwiederaufbau des Übertragungsnetzes (24. April 2020)*, § 4.1 - Voraussetzungen für die Aussetzung von Marktaktivitäten

In case the Creos network loses connection with the Amprion grid, it will be split automatically to allow, within the limits of available capacity, the power supply of the southern part of Luxembourg, including the City of Luxembourg, via the Elia grid in Belgium. The rest of the country will be in a state of blackout (cf. section 1.2 of the system restoration plan).

If the restoration plan is triggered, regional dispatching (e.g., medium voltage grids) is subordinated to the Creos control centre, which is also responsible for the coordination with the Amprion control centre, the Elia national and regional control centres, and the dispatching of the Sotel industrial grid. The lines of communication are secured and will also work in the event of a blackout (cf. section 1.2 of the aforementioned plan).

Creos' restoration procedures include decision-making schemes to guide operators through the different phases of recovery. These schemes avoid neglecting important elements, allow for working in a structured manner and ensure that all the information necessary to be able to choose the most appropriate strategy is evaluated. The documentation of the process will form the basis of the ex-post analysis of the crisis, whose results will provide valuable elements for a better understanding of the crisis and for improving procedures and the restoration plan (cf. section 3.1 of the aforementioned plan).

In the event of a solar storm which can be forecasted by Space Agencies a few days in advance, it may be appropriate to initiate a voluntary (partial) blackout in order to protect the grid and power generation centres from the damaging consequences. As a voluntary blackout is a coordinated process, the restoration procedure after the event may be simpler to manage compared to an uncontrolled state of emergency. Nevertheless, it would follow the same procedures laid out in the system restoration plan.

3.1.4 Information

In all phases of the crisis management, the flow of information plays a decisive role. The internal communication serves to keep all relevant bodies informed and coordinated, and provides the basis for deciding and approving on the most sensible measures. External communication, i.e. specifically the transparent information towards the public, serves to strengthen the trust in the respective strategy of crisis management and to avoid irrational behaviour.

3.1.4.1 *Procedures and measures by the government and public authorities concerning information flows*

On a government level, the procedures related to information flows are defined in the respective emergency response plans.

According to section 5 of the ***Emergency response plan for an outage of energy supply***, the main procedures of internal communication for any kind of electricity crisis are as follows:

- The system operator alerts the head of cell for the evaluation of the risk for an outage of energy supply as soon as the system operator becomes aware of a major incident or attack.
- The High Commissioner for National Protection is alerted if the incident is likely to have a significant impact.
- The Prime Minister and Minister of State is alerted.

The information of the public is provided by the cell for communication and information. Based on the communication strategy the public is informed of

- the incident or attack and its impacts,
- the emergency plan in the event of an attack or technical fault in energy supply system,
- the establishment of the crisis cell including its composition and missions,
- the measures taken by the relevant authorities,
- the behaviours to be adopted by the population, and
- the stages of restoration of supply.

This information is spread through communication channels defined in the crisis communication strategy such as radio, TV, print media, website (in particular www.infocrise, hotlines, social networks, etc., provided that these channels are still available.

According to the ***Emergency response plan for an attack against or the outage of information systems***, the internal communication procedures are triggered as soon as any national or international actor reports a major cyber incident to the relevant Luxembourg authorities (cf. section 3 of the aforementioned plan).

- The cyber risk assessment cell is informed about the incident or attack.
- The High Commissioner for National Protection is alerted if the incident is likely to have a significant impact.
- The Prime Minister and Minister of State is alerted.

The public is informed of developments by the government (cell for communication and information) through the communication tools as described for the response plan for an outage of energy supply (cf. section 6 of the aforementioned plan).

According to section 2.1 of the ***Emergency response plan in the event of a nuclear accident***, the internal information procedure comprises the following three elements:

- The radiological evaluation cell is alerted as soon as the information of the incident is available.
- The High Commissioner for National Protection is alerted if the accident is likely to pose a danger to the population.
- The Prime Minister and Minister of State is alerted.

The crisis cell informs the public of all protective measures, recommendations and bans at the necessary time via the press, social media and the website www.infocrise.lu (cf. section 5 of the aforementioned plan). Furthermore, it directs CGDIS to activate specific warning signals through the national siren network, as described in Section 2.5 of the aforementioned plan).

3.1.4.2 Procedures and measures by system operators concerning information flows

In case that the system operator has activated measures according to the ***System Defence Plan***, the system operator in charge of the coordination informs the Government Commissioner of Energy and the Institut Luxembourgeois de Régulation (ILR), as well as the High Commissioner for National Protection in writing of actions and measures.

In case of a prolonged situation, the affected system operators inform their customers of the decisions made, and in particular of the expected duration of the crisis situation.

In case of national disconnection, the TSO informs the public through appropriate communication channels.

3.2 Regional and bilateral cooperation

Luxembourg is involved in several arrangements aiming at regional and bilateral cooperation on both a government as well as a system operator level. Some of these arrangements are of binding nature and define procedures for mutual support in specific crisis and emergency situations, while others are activities to contribute actively to achieve further progress related to risk preparedness in the energy sector and other fields of international interests.

3.2.1 Overview of regional and bilateral cooperation

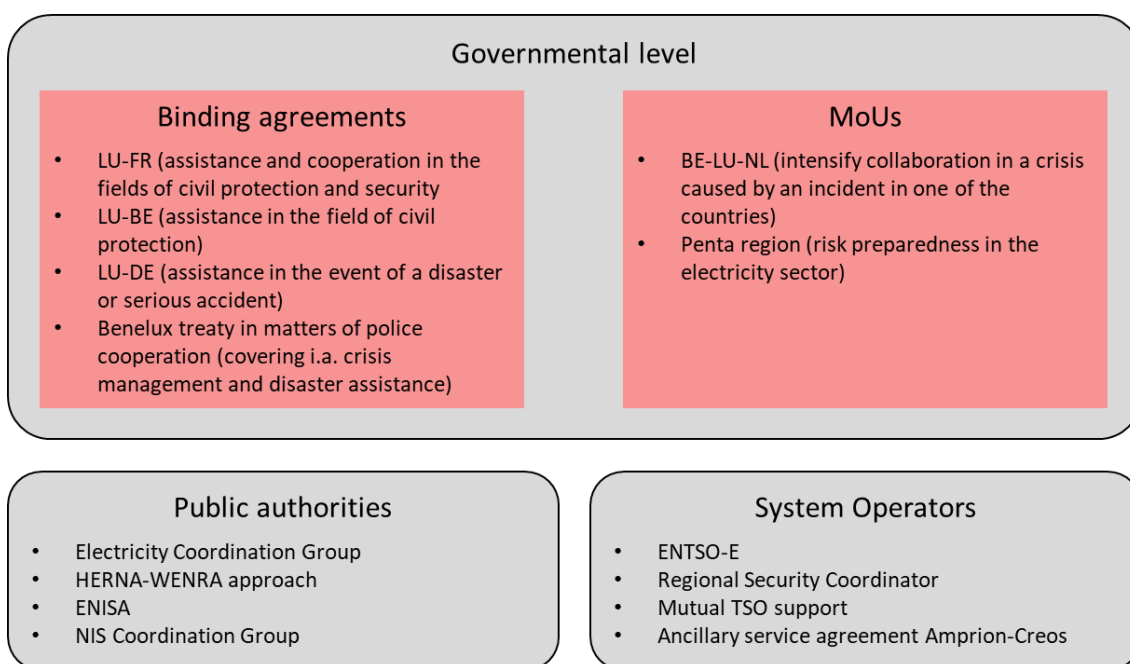


Figure 3: Arrangements related to bilateral and regional cooperation

3.2.2 Mechanisms for regional and bilateral cooperation

3.2.2.1 Cooperation on a governmental level

Luxembourg has concluded several binding intergovernmental agreements in the context of managing crisis situations with potential cross-border consequences. These agreements comprise:

- The **Agreement between Luxembourg and France on assistance and cooperation in the field of civil protection and security** (act of April 2016) for the implementation of voluntary and mutual assistance in the event of a disaster or serious accident requested either through diplomatic channels or by the respective competent authority.
- The **Agreement between Luxembourg and Belgium on mutual assistance in the field of civil protection** (act of August 2016) in the event of a disaster or serious accident, especially incidents of chemical and nuclear nature.
- The **Agreement between Luxembourg and Germany on mutual assistance in the event of a disaster or serious accident** (act of December 1981).

- The ***Treaty between Belgium, Luxembourg and the Netherlands in matters of police cooperation*** (July 2018).

The assistance foreseen in these agreements generally consists in the following aspects:

- sending rescue teams,
- providing equipment,
- transmitting information.

The agreements typically foresee cooperation covering:

- measures to predict and prevent major natural and technological hazards including but not limited to the hazards identified in section 1.2.,
- protecting and safeguarding people, property and the environment threatened by a major natural or technological disaster,
- training for civil protection and security actors,
- mutual assistance in the event of disasters or serious accidents,
- mutual assistance between emergency services on both sides of the border
- methodologies for the establishment of contingency plans,
- the study of common interest problems in forecasting, prevention, assessment and management of emergencies,
- exchanges of experts and specialists, and
- exchanges of information and documentation on civil protection and security.

Different working groups for crisis management and disaster assistance (e.g. “SENN-CRISE”) enable the cooperation within the **Benelux** union and with Germany. The main pillars are the collaboration of national crisis cells, improvement of communication against the background of specific crisis scenarios and common exercises to ensure a smooth communication flow during a crisis.

These binding agreements are complemented by the following MoUs:

- The ***Memorandum of Understanding between Belgium, Luxembourg and The Netherlands***²² from June 2006 to intensify their collaboration in a crisis caused by an incident in the territory of one of the countries. The cooperation covers the coordination of national policies as well as planning and execution of countermeasures. This coordination is established inter alia by risk identification, planning of civil protection measures, crisis management, mutual assistance on an ad-hoc basis, exchange of information, and communication with the public and corporate exercises.
- Pursuant to the requirements on solidarity and regional cooperation, the Pentalateral Energy Forum drafted and signed a ***Memorandum of Understanding on risk preparedness in the electricity sector*** in December 2021, which can be found in annex A of this plan. It provides a common understanding and clear mandate to continue the collaboration concerning the identification of possible common measures.

The common measures that will be assessed in further detail within the Penta Context will build upon existing inter-TSO agreements, as well as other relevant solidarity mechanisms. Examples of such existing mechanisms are the network code on electricity emergency and restoration or the guideline on electricity transmission system operation. More specifically,

²² Original title *Le Mémorandum d'Accord concernant la coopération dans le domaine de la gestion des crises pouvant avoir des conséquences transfrontalières entre le Royaume de Belgique, le Royaume des Pays-Bas et le grand-duché de Luxembourg*

possible common measures that will be analysed in more detail are: 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. Within the context of Support Group II of the Pentalateral Energy Forum dealing with security of supply, a preliminary exchange on these measures already took place. Based on the mandate and intentions expressed in the MoU, they will be further analysed from a regional point of view with respect to their technical, legal and economic characteristics.

3.2.2.2 Cooperation between public authorities

In the framework of international collaboration related to security of supply on European level, the **Electricity Coordination Group** is a forum for the exchange of information and coordination of electricity policy measures having a cross-border impact. It also shares experiences, best practices and expertise on security of supply in electricity, including risk-preparedness, generation adequacy and cross-border grid stability, and assists the European Commission in designing its policy initiatives. The group's members represent national government authorities, in particular ministries responsible for energy; national energy regulatory authorities for energy; the Agency for the Cooperation of Energy Regulators (ACER), and the European Network of Transmission System Operators for Electricity (ENTSO-E).

For the particular risk of nuclear incidents, Luxembourg is also involved in the Europe-wide **HERNA-WENRA approach**, which comprises the necessary mechanisms for countries to exchange adequate information and to achieve practical and operational solutions on a voluntary basis during a nuclear accident. This approach aims to establish a uniform way of dealing with any serious radiological emergency situation, regardless of national borders, hence allowing for coherent and coordinated protective actions.

With regards to cyber related risks, cross-border cooperation is guaranteed and cross-border assistance is possible both at the **CERT** level and within the framework of international organisations of which the Grand Duchy of Luxembourg is a member (European Union, Benelux, NATO, UN, OSCE). In particular, the **European Union Agency for Cybersecurity (ENISA)** pays attention to a common strategy to strengthen Europe's preparedness and response capabilities to cyber incidents and to improve cyber security.

Furthermore, the **NIS Cooperation Group**, which regroups representatives of the EU Member States, the European Commission and ENISA, was established by the NIS Directive to foster cooperation in view of achieving a high common level of security for network and information systems in the European Union. It supports and facilitates the strategic cooperation and the exchange of information among EU Member States. On the operational side, the NIS Cooperation Group is supported by the work of the network of Computer Security Incident Response Teams (CSIRTs network), dedicated to sharing information about risks and ongoing threats and cooperating on specific cybersecurity incidents. The CSIRTs network was established under article 12 of the NIS Directive, which also defines its role. The NIS Cooperation Group provides strategic guidance for the activities of the CSIRTs network. The NIS Cooperation Group is also working closely with the European Cooperation Network on Elections to counter threats to electoral processes under a new joint operational mechanism set-up as a part of the European Democracy Action plan. As the national competent authority for Luxembourg for implementing the NIS Directive, the national regulatory authority ILR represents Luxembourg in the NIS cooperation group.

3.2.2.3 Cooperation between system operators

ENTSO-E, the European Network of Transmission System Operators for Electricity, is the association for the cooperation of the European TSOs. Member TSOs are responsible for the secure and coordinated operation of Europe's electricity system. ENTSO-E's key responsibilities include the following:

- Development and implementation of standards, network codes, platforms and tools to ensure secure system and market operation as well as integration of renewable energy
- Assessment of the adequacy of the system in different timeframes
- Coordination of the planning and development of infrastructures at the European level (Ten-Year Network Development Plans)
- Coordination of research, development and innovation activities of TSOs
- Development of platforms to enable the transparent sharing of data with market participants.

Regional mechanisms to ensure an appropriate reaction at regional level are provided by the **Regional Security Coordinators (RSC)**. In accordance with article 35 of **Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity**, the existing RSCs will be replaced by Regional Coordination Centres (RCCs) as of 1 July 2022.

Creos is a customer of the RSC TSCNet Services²³.

RSCs are entrusted with a set of mandatory services for their customers according to EU legislation:

- **Establishing a common grid model:** the establishment of a common grid model (CGM) is the basis for every single evaluation of transmission system security. The European CGM is tailored to the requirements of the most important services of an RSC and consists of detailed input and forecast data on generation, consumption, and network connectivity for all TSOs. The data is provided by the TSOs in the form of their individual grid models (IGMs) and other specific information. The RSC must check the quality of the IGMs and integrate them into the CGM in accordance with predefined rules.
- **Coordinated security analysis:** the aim of the coordinated security analysis is to identify possible security restrictions after the market closure based on the so-called (n-1) security principle in the framework of the day-ahead congestion forecast (DACF) and intraday congestion forecast (IDCF) processes. If security restrictions are detected, countermeasures can be identified and validated with the affected TSOs. For example, switching configurations can be changed based on results of an outage planning coordination process, tap positions of phase-shifting transformers can be changed or redispatch actions can be done, even if they cover complex security restrictions that require corrective measures in the networks of more than two TSOs at the same time (Multilateral Remedial Actions). The decision-making process between TSOs is organised via teleconferences.
- **Coordinated capacity calculation:** in its function of coordinated capacity calculator, the RSC calculates the cross-border transmission capacities for each relevant Capacity Calculation

²³ Further shareholders and customers of TSCNet Services can be found on TSCNET's website www.tscnet.eu.

Region (CCRs) based on the methods approved by the national regulatory authorities and a tailor-made common network model.

- **Outage planning coordination:** the process collects all planned shutdowns of transmission and relevant generation elements and evaluates whether their simultaneous overlay meets the requirements for system security. If necessary, the RSC identifies and coordinates remedial actions with the TSOs and other RSCs in order to optimise the outage plans and to ensure that the planned measures are implemented as effectively as possible. The final outage plan is incorporated into the coordinated security analysis and capacity calculation processes.
- **Short and medium-term adequacy forecasts:** a secure supply requires the availability of a minimum of installed generation capacity in order to reliably provide the necessary supply capacity. TSOs need an early assessment of whether market liquidity is limited or whether the regional distribution of generation capacity and consumption leads to congestion in order to prepare for such an exceptional situation. The RSC provides detailed and continuously updated short and medium-term adequacy forecasts based on information on the availability, consumption and expected state of transmission corridors with forecast horizons between weeks and a few days in advance. The results are discussed in a weekly operational planning teleconference.
- **Consistency check of TSOs' system defence and restoration plans:** application of common grid operation rules shall prevent the power grid from reaching an emergency state or from suffering a power failure. TSOs are obliged to take care of these unlikely situations and to draw up system defence and recovery plans in order to maintain and restore the functioning of the transmission grid. The RSC reviews the TSOs' restoration plans for consistency and provides a technical report for all TSOs to be forwarded to the national regulatory authorities and ENTSO-E to monitor the implementation.

In addition to European cooperation, mutual TSO support is in place on a bilateral and regional basis, based on the following technical measures in case that national measures are not sufficient to fully mitigate the respective crisis:

- If critical assets of the electricity system fail, e.g. due to attacks or extreme weather, parts of the transmission grid of Luxembourg and connections with Germany, Belgium, and France can be reconfigured to preserve system stability (cf. **System Defence Plan** and explanations provided in section 3.1.3.2). Through the possibility to use foreign grid infrastructure more extensively, this measure allows for a more flexible load flow control and shall prevent severe overloads in the region. This measure would also be applied as coordinated preventive action in case that the results of the network security analyses performed by the RSC point to the necessity of suitable regional measures.

The mechanism of mutual TSO support in emergency situations is part of the **Network Code E&R**.

- As Luxembourg and Germany form a common electricity market, **Rules for Market Suspension and Restoration** include closely coordinated processes between all TSOs in the two countries (cf explanations in section 3.1.3.2).
- In the case that preventive and corrective measures have not been successful and the system falls into a blackout condition, a structured restoration of energy supply is initiated. This process is in the first instance based on the national **Grid Restoration Plan**. As laid down in the **Network Code E&R**, these restoration plans shall be harmonised to ensure their

effectivity also on regional level and to consider mutual support or even to handle cases where a national system is in principle not capable to recover energy supply on its own (cf. section 3.1.3.2).

Creos and Amprion have an ancillary service agreement in the context of load-frequency control and system restoration. As described in sections 3.1 and 3.2 of the **System Defence Plan** and in section 1 of the **System Restoration Plan**, Creos appointed Amprion as LFC area operator for the common load and frequency control area of Amprion and Creos in accordance with article 120 of the **System Operation Guideline**. Furthermore, section 3 of the **System Restoration Plan** sets out that the agreement covers the procurement of ancillary services by Amprion including black start and support in a blackout situation in Luxembourg.

4 Crisis coordinator

The execution of the **Emergency response plan for an outage of energy supply** is the responsibility of the **Prime Minister and Minister of State** and of the **Minister of Energy**. The crisis cell is activated by the **Prime Minister and Minister of State**. The **High Commission for National Protection** ensures coordination at the operational level related to the prevention, anticipation and management of crises.

Prime Minister and Minister of State

Xavier Bettel

Ministère d'État
2, place de Clairefontaine
L-1341 Luxembourg
Luxembourg

Phone: (+352) 247-82100

Fax: (+352) 461720

Email: ministere.etat@me.etat.lu

Web: me.gouvernement.lu

Minister of Energy

Claude Turmes

Ministère de l'Énergie et de l'Aménagement du territoire
4, place de l'Europe
L-1499 Luxembourg
Luxembourg

Tél. (+352) 247- 74606

Fax (+352) 247-84311

Email: secretariat@energie.etat.lu

Web: www.mea.gouvernement.lu

High Commission for National Protection

Haut-Commissariat à la protection nationale

Centre national de Crise

46, rue du Château

L-6961 Senningen

Luxembourg

Tél. (+352) 247-88900

Fax (+352) 247-88910

Email: secretariat@hcpn.etat.lu

Web: www.hcpn.lu

5 Stakeholder consultations

The MEA, in its role as competent authority for the Regulation, closely collaborated with the High Commission for National Protection HCPN and TSO Creos during the complete process of preparing the Luxembourg risk preparedness plan for the electricity sector.

For the identification of national crisis scenarios, MEA consulted the transmission and distribution system operators, relevant energy suppliers, the High Commission for National Protection HCPN as well as the national regulatory authority ILR. They were invited to participate in a workshop with the goal to introduce and discuss the proposed national electricity crisis scenarios. The workshop was followed by a consultation phase of two weeks giving the stakeholders the opportunity to further comment on the proposed scenarios in writing. The results of the consultation were integrated in a slightly revised list of national crisis scenarios.

Before submission to the European Commission and the Electricity Coordination Group early April 2021, the **draft plan was consulted with the most relevant stakeholders**, i.e., the High Commission for National Protection HCPN, the national regulatory authority ILR, as well as the TSO Creos. Comments and proposals for improvement have been collected during a period of 2 weeks, and a dedicated workshop was organised to exchange in detail on the draft plan. Comments and proposals received were categorised and appropriately considered for the final version of the draft plan. Due to time constraints, an additional consultation with a broader set of stakeholders could only be initiated subsequent to the submission of the draft plan on 5 April 2021, inviting the HCPN, ILR, the transmission and distribution grid operators, all suppliers active in the Luxembourg electricity market, relevant producers, the Union of Consumers (Union Luxembourgeoise des consommateurs nouvelle ASBL, ULC) as well as the Federation of Luxembourgish Industrials (Fédération des Industriels Luxembourgeois, FEDIL) to share their comments on the draft plan during a period of one month (1-30 June 2021). A Webconference was held on 14 June 2021.

On a **regional level**, the **Pentalateral Energy Forum** organized 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 organized in June 2021, to exchange initial concerns and make clarifications. To align this initiative with the activities on a European level, the European Commission was invited to attend the meeting, and a representative of the Forum was available shortly after to give a presentation of the main results of the outcomes of the

regional assessment during a dedicated meeting of the Electricity Coordination Group in June 2021.

The outcomes of this meeting will be 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 Directors-General at the end of June. Afterwards, Penta-members had until mid-July to file written comments to the draft national Risk Preparedness Plans. Member States took these comments into account while finalizing their Risk Preparedness plans.

6 Emergency tests

Crisis prevention and management on bilateral or regional level require seamless coordination and communication under the responsibility of the crisis coordination entity. On the level of system operators, emergency tests are executed regularly, as outlined in the **Creos Test Plan**²⁴ according to article 43 of **Regulation EU 2017/2196**. The requirements for compliance testing of capabilities are defined in the section “Compliance and review” where each TSO shall periodically assess the proper functioning of all equipment and capabilities considered in the system defence plan and the restoration plan involving all relevant distribution system operators and defence/restoration service providers.

The **Creos Test Plan** comprises the following compliance tests:

- Under-frequency disconnection relays are tested during the commissioning phase to verify the compliance of newly installed equipment. The test is repeated every 5 years.
- Production facilities (incl. batteries) are tested whether they are able to reduce their active power infeed if the frequency is above 50.2 Hz following a static given by Creos. The facilities must also be able to inject the maximum active power if the frequency drops below 49.8 Hz. This test is to be carried out during commissioning or after any intervention on equipment that has an impact on this ability to adapt the active power according to the frequency of the network, respectively.
- Blocking the automatic tap changing of power transformers is a measure to prevent a collapse of the network voltage and thus avoid a blackout. The compliance test of this functionality is carried out annually.
- Annual testing of generators and batteries to ensure continuity of control of substations being a relevant element in a potential grid reconstruction procedure.
- Testing of critical IT and telecommunications systems and installations related to availability and operation is performed at least every 3 years.
- The backup dispatching transfer procedure is tested annually.
- Simulator tests of the reconstruction plan as well as dispatcher training in the application of the procedures established by the reconstruction plan at least every 5 years.

²⁴ Original title *Plan d'essais de Creos Luxembourg SA, en sa qualité de gestionnaire de réseau de transport, conformément à l'article 43, paragraphe 2 du règlement (UE) 2017/2196 de la commission du 24 novembre 2017 établissant un code de réseau sur l'état d'urgence et la reconstitution du réseau électrique*

Restoration of the Luxembourg transmission grid cannot be achieved without support provided by the neighbouring TSOs Amprion (Germany) or Elia (Belgium), respectively. For this reason, **bilateral tests and trainings** related to restoration procedures are periodically performed.

Further obligations to pursue **inter-TSO trainings** related to aspects of real-time operation to consolidate and improve communication and coordination are defined in the SO GL.

On a **regional level**, 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 power 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 and 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, Penta members acknowledge the importance of continuing to regularly organize joint exercises. Based on the MoU signed in December 2021 and 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. The specifics of the upcoming joint exercises have been drafted and aligned within Support Group II during the finalization of the Risk Preparedness Plans.

A Memorandum of understanding of the Pentalateral Energy Forum on risk preparedness in the electricity sector

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 1st of December of the year two thousand and twenty one.

For the Kingdom of Belgium



For the Republic of Austria



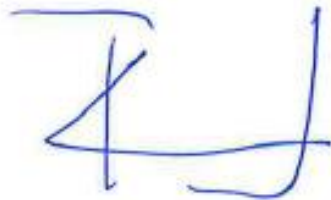
For the French Republic



For the Federal Republic of Germany



For the Grand Duchy of Luxembourg



For the Netherlands



For the Swiss Confederation



B Overview of reference documents

- **Bericht über die Versorgungssicherheit im Strombereich in Luxemburg**
available at <https://mea.gouvernement.lu/dam-assets/energie/electricite/VS-Bericht-Strom-2020.pdf>
- **Bestimmungen für die Aussetzung und Wiederaufnahme von Marktaktivitäten und die Bestimmungen für die Abrechnung im Falle einer Aussetzung von Marktaktivitäten gemäß Artikel 36 Abs. 1 und Artikel 39 Abs. 1 i.V.m. Artikel 4 Abs. 2 e und f der Verordnung (EU) 2017/2196 der Kommission vom 24. November 2017 zur Festlegung eines Netzkodex über den Notzustand und den Netzwiederaufbau des Übertragungsnetzes (24. April 2020)**
available at https://www.bundesnetzagentur.de/DE/Beschlusskammern/1_GZ/BK6-GZ/2018/BK6-18-289/BK6-18-289_beschluss_vom_04.08.2020.pdf?__blob=publicationFile&v=1
- **Business continuity plans**
non public
- **Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation**
available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R1485>
- **Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC**
available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012L0018>
- **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**
available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0944>
- **Electricity system defence plan of the Grand Duchy of Luxembourg**
consultation document available at https://www.creos-net.lu/fileadmin/dokumente/NEWS/pdf/2020-2022/System_defence_plan_Luxembourg_-_28_November_2019_-_v1.4.2.-signature_m%C3%A0j2021_final.pdf
- **Hochwasserrisikomanagementplan 2021-2027**
consultation document available at <https://eau.gouvernement.lu/dam-assets/administration/documents/projekthochwasserkaarten2021/hwrmp2021/Entwurf-Hochwasserrisikomanagementplan-2021-2027.pdf>
- **Loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité**
available at <https://legilux.public.lu/eli/etat/leg/loi/2007/08/01/n13/jo>
- **Loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale**
available at <https://legilux.public.lu/eli/etat/leg/loi/2016/07/23/n1/jo>
- **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**
available at https://nra.acer.europa.eu/en/Electricity/CLEAN_ENERGY_PACKAGE/Documents/Methodology%20to%20Identify%20Regional%20Electricity%20Crisis%20Scenarios%20in%20accorda

nce%20with%20Art%205%20of%20the%20Regulation_200106_submitted%20to%20ACER.pdf

- **Network development plan**
available at https://www.creos-net.lu/fileadmin/dokumente/NEWS/pdf/2020-2022/20210820_Network_Development_Plan_2040_-_HV_Transport_Grid_final_.pdf
- **Plan d'essais de Creos Luxembourg SA, en sa qualité de gestionnaire de réseau de transport, conformément à l'article 43, paragraphe 2 du règlement (UE) 2017/2196 de la commission du 24 novembre 2017 établissant un code de réseau sur l'état d'urgence et la reconstitution du réseau électrique**
consultation document available at https://www.creos-net.lu/fileadmin/dokumente/NEWS/pdf/2020-2022/210301_Plan_d_essais_Creos_Projet_v1_-_ILR2_-_SH_CB_final.pdf
- **Plan de reconstitution du réseau électrique**
available at https://www.creos-net.lu/fileadmin/dokumente/NEWS/pdf/2020-2022/Draft_Plan_de_Reconstitution_Vers_3_2020_final.pdf
- **Plan d'intervention d'urgence (PIU) "Rupture d'énergie"**
available at www.infocrise.lu
- **Plan d'intervention d'urgence (PIU) en cas d'urgence nucléaire**
available at www.infocrise.lu
- **Plan d'intervention d'urgence (PIU) "Cyber"**
available at www.infocrise.lu
- **Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection**
available at <https://legilux.public.lu/eli/etat/leg/rgd/2012/03/12/n1/jo>
- **Règles régissant le règlement des déséquilibres de l'énergie d'équilibrage en cas de suspension des activités de marché**
consultation document available at https://www.creos-net.lu/fileadmin/dokumente/NEWS/pdf/2020-2022/210322_ER_Creos_Doc_consultation_R%C3%A8gles_de_suspension_march%C3%A9.pdf
- **Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration**
available at https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2017:312:TOC&uri=uriserv:OJ.L_.2017.312.01.0054.01.ENG
- **Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity**
available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0943>
- **Risk-Preparedness Regulation – Identification of Regional Electricity Crisis Scenarios**
non public
- **Stratégie d'adaptation aux effets du changement climatique pour le Grand-Duché de Luxembourg**

B Overview of reference documents

available at https://environnement.public.lu/dam-assets/documents/klima_an_energie/Strategie-Adaptation-Changement-climatique-Clean.pdf

- **Stratégie nationale de cybersécurité IV (2021-2025)**

available at <https://cybersecurity-luxembourg.com/strategy>