NATIONAL RISK-PERPAREDNESS IN THE ELECTRICITY SECTOR - SPAIN

Objective

The purpose of this plan is to set down the measures that must be carried out and the parties that must take part when adressing the electricity sector crises foreseen for Spain

Tabla de contenido

Introduction.

The purpose of this document is to comply with the obligations set in articles 10, 11 and 12 of 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.

The Spanish Risk-preparedness in the Electricity Sector Plan is established as the instrument that includes all national, regional and even bilateral measures to be carried out in order to address the risks and consecuences derived from the differente electricty crises.

Article 16 of Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 also sets that all measures taken to prevent or mitigate electricity crises shall comply with the rules governing the internal electricity market and system operation.

In relation to this, on the one hand, a description of the measures that meets the requirements of transparency, clarity, proportionality and non-discrimination has been included.

On the other hand, and without prejudice to previous considerations, such transparency must also take into accounta that in certain cases the nature of the information is confidential for internal security reasons.

Finally, providing a description down to the last detail would lead to an inoperative and unmanageable plan beacuse of its sheer volume.

In this plan, all these considerations have been taken into account when drafting the specific measures described in it.

Finally, for the preparation of this document, as established in article 10.1 of Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019, the competent authority has consulted different parties which include the Transmission System Operator, to relevant Distribution System Operators, relevant energy producers and generators or their associations, and to the National Regulatory Autohority, when it is not the competent authority.

Plan Structure

The content of this Plan is aligned with articles 10, 11 and 12 of Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019, as well as with its Annex.

The Plan is structured as follows:

I. The first section includes a summary of the different crises scenarios identified at national level, including the different hypotheses and considerations taken into account when establishing them as the most likely electricity crises for Spain. It also includes those considerations related to possible regional impacts of those scenarios.

II. The second section is dedicated to the legal framework of the Plan, both at EU level as well as at national level. It includes aspects that range from its most basic fraemwork precepts to those that regulate the most practical, inmediate and operative aspects. This section seeks to include the most comprehensive reference posssible to the different regulations, rules and norms, so that it compiles all the necessary regulatory authorizations enjoyed by the different subjects that participate in it, as well as the actions that must be taken in its execution.

    In this sense, on the one hand, the plan takes into account other legal frameworks that beyond that of the electricity sector, such as those that regulate matters like critical infrastructures.

    On the other hand, the range of references made goes from the most basic or general framework, to those specific developments set in order to achieve the most operational and action parts within the plan.

III. Thethird section describes the parties who act and have responsibilities in the plan. Within this section, a description is included of the 3 large groups and individual parties that act in the Plan. A specific reference is also made to the Competent Authority.

IV. The fourth section sets the planned procedures and actions that are to be carried out in the different scenarios, including preventive and preparatory actions.

1. Electricity crisis scenarios.

Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 defines an electricity crisis as *"a present or imminent situation in which there is a significant electricity shortage, as determined by the Member States and described in their risk-preparedness plans, or in which it is impossible to supply electricity to customer"*

To address these crises, it is necessary to first properly identify them, carry out a detailed analysis of them and finally perpare for their development and potential impacts.

This chapter proceeds to identify for Spain the different national and regional crisis scenarios considered, and then justify said identification, describing in a summarized vesion the methodology used in this phase.

1.1 Identificaction of national crisis scenarios.

As set in article 6 of Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 the regional crisis scenarios were identified and set in the report *"Identification of regional electricity crisis scenarios"*, prepared by the European Network of Transport System Operators (ENTSOe). These scenarios have been taken as a starting point in this Plan.

The report established 31 possible scenarios that were grouped into 9 major categories, as shown below:

I. Cyberattacks:

a. *Cyberattack against entities connected to the electricity grid* - which is an attack against ICT systems, belonging to either the TSO[1], to one or more DSO[2], or to generation plants or large consumers.

b. *Cyberattack against entities not connected to the electricity grid* – which is an attack against the ICT systems of subjects of the electricity market not phisically nor directly connected to the networks (eg. market platforms, etc.)

II. Attacks:

a. *Physical attack on critical infrastructures* - consists of an attack of a physical nature making use of the vulnerabilities of power lines, transformers, substations, generation plants and/or data centers.

b. *Physical attack on control infrastructures* - consists of an attack of a physical nature making use of the vulnerabilities of the main or reserve control centers of the TSO, of the relevant DSOs or of the operations centers of the main generation plants.

c. *Threat to key personnel* - In this situation those affected are part of key personnel (e.g., system operators, ICT service administrators, high-ranking privileged personnel, CEO, CFO, etc.) and they are forced to carry out actions that destabilize the system.

d. *Insider attack* - this is sabotage carried out by one or more employees of the company itself or of subcontractors through physical action or the improper use of ICT systems.

III. Extreme weather events:

a. *Solar Storm* - This is a Carrington like event. In these situations the sun produces a strong corona mass ejection (CME). The effects will be more noticeable in northern European countries, although there will also be significant impacts in central Europe. Space Agencies can predict these types of events a few days in advance.

b. *Storm* - consists of a situation in which a predicted storm increases in strength and extent within an hour. The size is such that it spans from Eastern Europe to

[1] Transport Systema Operator.
[2] Distribution System Operator.

Western Europe with an average wind speed of at least 150 km/h and gusts exceeding 200 km/h.

c. *Cold wave* - a wave occurs throughout Europe with temperatures between -10 and -20°C below the seasonal average, so that:

    i. Water reservoirs (lakes, rivers, swamps, etc.) freeze and reserves are depleted.

    ii. There is absence of wind.

    iii. Energy demand increases becuase of the cold, particularly in countries with a significant share of electric heating systems.

    iv. Energy generation decreases because of limitations in the capacity to cool thermal modules of the distribution/transmission networks (PGM). This is due to the fact that water/cooling liquid reserves are frozen and/or operational problems arise in module equipment and even coal may freeze in some countries.

    v. There are limitations in the generation because of limitations in the capacity to cool the generation modules due to the fact that water/cooling liquid reserves are frozen and/or operational problems arise in module equipment.

    vi. Hydroelectric generation decreases.

    vii. Due to weather conditions, some network elements may be suffer greater stress (due to freezing, etc.) and reliability may be reduced.

d. *Rainfall and flooding* - Heavy rains take place during several days causing flooding at substations and power plants.

e. *Winter incident* - in this situation there are multiple failures in overhead power lines as a result of the accumulation of snow or ice. This causes failures in insulating elements of the lines (OHL insulators) or in the physical fall of the cables. Tower failures (due to ice or snow accumulation) can lead to multiple shots on circuits. Snow avalanches in mountainous regions can also trigger multiple shots on circuits.

f. *Multiple failures due to extreme weather events* - the triggering event may be:

    i. Multiple failures caused by extreme weather conditions

    ii. A set or type of network components that begins to fail without warning due to a sudden heat wave in a short period of time, affecting power distribution.

g. *Heat wave* - a heat wave affects security of supply by:

    i. Decreasing capacity in generation facilities.

    ii. Causing sudden trips in several generation units due to insufficient cooling of generation modules.

A heat wave affects network security by:

i. Overloading certain elements that cause N-1 incidents as a result of failures.

ii. Limiting line capacity or increasing electricity demand due to the energy demand associated with air conditioning. The internal resources/reserves of different operators may also be affected.

A heat wave can be accompanied by incidents related to:

i. Capacity issues.

ii. Structural degradation.

iii. Stability problems.

h. *Drought* - low water levels give way to low hydroelectric production (with a critical number of hydroelectric facilities out of operation). Also, several thermal generation units may have to stop or reduce production becuase of limitations in cooling capacity.

IV. Natural disasters:

a. *Volcanic eruption* - this incident is triggered by an active volcano that is expected to produce a large amount of ash. Seismic activity in the vicinity is also expected before the eruption, although it is most likely with less than an hour's notice.

b. *Earthquake* - An earthquake of considerable magnitude may occur, damaging power transmission infrastructures or production facilities.

c. *Wildfire* - fires are started and spread by heat and wind. In some cases they cannot be controlled for weeks and are aggravated by punctual and strong summer storms (which are associated with strong winds and lightning that propagate or create new foci).

Uncontrolled forest fires can lead to unavailability or the inability to operate certain generation, transmission or distribution units/assets. Some possible consequences are:

i. Massive N-1 incidents that create a cascading effect.

ii. Structural degradation.

d. *Pandemic* - this is a spread of a disease on an international scale. TSO staff will be affected. The same can also happen with personnel in substations, production plants and DSOs to the point of not having enough human resources.

V. Fuel shortage

a. *Shortage of fossil fuel (including natural gas*) - the initiating event takes place over a year combining high demand for domestic fuel with low reserves. It can be one of the following cases:

i. Continued disruption in nuclear fuel production.

ii. Failure or shutdown in the fuel supply system, either technical or provoked.

iii. Limitation in supply for market, political, meteorological reasons.

iv. In the case of fuel imports, the transit states can even further limit available fuel in order to guarantee their own supply, which leads to a significant reduction in fuel for the affected generation plants.

This coincides with an inability to compensate for restrictions with supply form other sources/suppliers. Additionally, production from alternative manageable facilities or from importing energy may be restricted.

b. Nuclear fuel shortages - the trigger occurs during the year, when simultaneously there is a high demand for electricity and a reverse low of nuclear fuel. The causes can be:

i. Continued disruption in nuclear fuel production.

ii. Failure or shutdown in the fuel supply system, either technical or provoked.

iii. Limitation in supply for market, political, meteorological reasons that prevent the arrival of sufficient fuel to the affected nuclear plants

This coincides at a time of year when there is a high electricity demand. It can coincide with intermittent unavailabilities in both generation and interconnections.

VI. Human factor

a. *Human error* – the triggering vent may be:

i. Error by operators who disconnect an essential element from the network.

ii. Any violation of the N-1 criterion caused by human error.

b. Strike, riot, union action - the event that starts the crisis can be:

i. Disputes of some kind that escalate to actions in large industries or riots.

ii. Riots, blockades or social disturbances take place (regardless of reasons or causes).

One direct consequence is that personnel in the energy sector (in the mining, production, distribution or transportation of electrical energy) do not want to work or cannot access work.

VII. Market errors:

a. Unforeseen interaction of market rules - The trigger will be highly unusual and extreme behavior by some market parties (entering a market panic situation), possibly as a result of any of the following circumstances:

i. Changes in some market rules or mechanisms in at least one country that allow unwanted effects in the markets (such as gaming or arbitration that is detrimental to system or supply security).

ii. Highly unusual weather, demand or system conditions with which many market players are not familiar, such that:

1. Highly unusual weather conditions can mean very low or very high temperatures for 10 or more consecutive days

2. A highly unusual demand can be caused by a disturbance in demand that lasts more than 10 consecutive times and is caused by economic, social or political reasons.

When referring to electricity markets, all types of markets are considered, including wholesale, capacity mechanisms, emissions mechanisms, cross-border capacity mechanisms, etc.

Automated trading algorithms, if used in affected markets, can increase risk or accelerate crisis development.

b. *Unwanted electricity flows* - The initiating event is a higher-than-planned energy whisi is the result of increased production by renewables (solar and wind) and other external conditions, such as regional redispatches.

Uncoordinated large energy flows are regsitered, for example, when significant volume flows occur at national borders, and when N-1 criteria are not met and redispatches must be used.

VIII. Technical failures:

a. *Local technical fault* - The initiating event is a local technical fault with cross-border impact (incident more serious than an N-1 type):

i. Failure of a critical element (eg. a transformer, a component related to the system stability, etc.).

ii. Fire or explosions in a substation.

b. Loss of ICT systems in real time operation - in this type of crisis the triggering event can be:

i. Loss or unavailability of a substantial part of ICT infrastructure or telecommunications systems used in the systems of the electricity sector or the operation of the electricity market.

ii. Loss or unavailability of one or more ICT systems used in planning and real-time operation of the electrical system (e.g. systems for calculating the safety of grid operation, predictions of renewable generation, system measurements), including failures resulting from technical failures.

c. Multiple simultaneous failures - Some of the following failures occur:

i. Failures in HVDC cables that cause the disconnection of several production plants resulting in a lost power ratio that exceeds the thresholds of N-1 scenarios.

ii. Failures in substations or transmission/distribution lines that cause large-volume supply cuts to consumers.

iii. Simultaneous or very close in time failures in multiple computers that exceed safety thresholds and for which the system is not prepared.

iv. An unknown system threat. This threat can manifest itself as a consequence of offline tests not being sufficiently accurate or because the scenario in question was not studied.

v. An unknown system threat derived from poor measurement operation, caused by poor performance of monitoring equipment.

vi. Violation of security standards/protocols as a result of an operational error or because control response was not fast enough to preserve system security.

vii. Multiple failures in network assets that cause the separation of a part of the system with insufficient generation capacity.

viii. Short circuits

d. *Cascading or serial failures of equipment* - Some of the elements of the transmission or distribution networks begin to show anomalous behaviors that increase the risk of failure or that lead to such failures.

In some cases, analysis makes it possible to discover that the cause is a systematic, manufacturing, installation or maintenance defect (weak towers, faulty components in circuit breakers throughout the series, in particular short-circuit breakers, installation of algorithms protection errors, etc.). Thus all elements of the same type/lot are liable to suffer the same failure/defect.

All suspicious items are considered unsafe, but cannot be replaced, turned off, or repaired.

The problem can be detected in one Member State, but it is likely to affect others at the same time, since the suppliers may be the same.

IX. Other crises scenarios:

a. *Electrical system control mechanism complexity* - The trigger for this type of crisis is technical failures in the ICT systems, in the communication systems or that a network protection component sends a signal to other networks, production units or component of the control centers that gives rise to a cascade failure, as a consequence of the high interdependence of highly complex systems.

b. *Industrial/Nuclear Accident* - A serious industrial accident occurs (such as a radiological pollution release resulting from an explosion at a nuclear plant or the emission of toxic pollutants from a chemical plant for a variety of reasons (technical failure, earthquake, sabotage / attack terrorist, human error, etc.).

c. *Unusually large error in the renewables share predictions* - the initiating event is a considerable difference between real and predicted generation by renewable

units (solar or wind), due to unusually large errors in prediction, errors in forecast data itself or due to rapid and unforeseen changes over time.

With the participation and contributions of different parties of the electricity system, other interested parties, as well as the CNPIC, in December 2020 the following 8 National Electricity Crisis Scenarios and their variants (in the case of cyberattacks) were identified:

1. **PANDEMIA**
2. **TORMENTA EXTREMA**
3. **CIBERATAQUE:**
    i. **Ciberataque a los Sistemas de Control**
    ii. **Ciberataque a equipos críticos de control, protecciones y telecomunicaciones**
4. **ATAQUE FÍSICO A CENTRO DE CONTROL**
5. **ATAQUE FÍSICO A ACTIVOS CRÍTICOS**
6. **INCENIDO O EXPLOSIÓN EN UN ACTIVO CRÍTICO**
7. **SABOTAJE POR PARTE DE PERSONAL INTERNO**
8. **INCENDIO FORESTAL**

1.2 Regional crisis scenarios.

An electricity supply crisis can have a regional impact when it is a cross-border event by its very nature, since it is a large-scale event, or when, in the case of a national crisis, the event has cross-border consequences and impacts. On practical terms, a regional crisis scenario is understood as one that affects two or more Member States.

Taking into account that electricity markets and systems are interconnected, preventing and managing electricity crises cannot be considered an exclusively national task. Therefore, it is necessary to foresee and take advantage of the possibility of adopting more efficient and less costly measures in a framework for effective regional cooperation.

In the first place, the concept of *"region"* is included and applied in Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 and must be taken into account in order to face crises with an impact that goes beyond one's borders. of the Member States.

Applying the criteria and indicators set out in Annex II of the methodology to identify regional electricity crisis scenarios, the following 7 crisis scenarios have been identified from those foreseen for Spain with a possible cross-border impact:

1. Pandemic (taking as an eample the 2009 Flu A and more recently the COVID-19).
2. Extreme storm (taking the 2020 Storm Glory as an example).
3. Cyberattack (in its two variants of attack on control centers and/or attacks on critical facilities of the Transport Network).
4. Simultaneous attack on several critical electrical substations.
5. Insider sabotage (either own personnel or belonging to one of the contractors).
6. Supply problems of natural gas (eg Russia - Ukraine supply cut 2004 and 2014).
7. Large system imbalance.

Interdependence between the electricity systems of the different Member States is such that this factor must be taken into account when preparing for crises that may affect any one country.

That is why, in each of the anticipated national crisis scenarios, assessments of cross-border impacts are included, as well as the responses and other additional actions that may be taken within the framework provided for coordination with the rest of the affected countries.

1.3 Methodology and justification for the identification of national crisis scenarios.

In order to determe which are the electricity crisis scenarios that should be taken into account in this plan, an analysis and evaluation procedure of the 31 proposals described in point 1.1 of this plan has been carried out.

The scale of assessment of the scenarios used has taken into account two aspects related to crises:

- The probability of a crisis occurring.
- The impact of that crisis.

In relation to the **probability of their occurrence**, crises are classified as:

I. **Very likely** - if they are expected to take place almost every year. Specifically, the frequency of occurrence is greater than 0.5 per year or the maximum time between events is less than 2 years.

II. **Probable** - if it is estimated that they will take place approximately every two years. Specifically, the frequency of occurrence is between 0.2 and 0.5 per year or the maximum time between events is in the range of 2 to 5 years.

III. **Possible** - if the crisis is viewed as a potential threat. In this sense, the frequency of occurrence is between 0.1 and 0.2 per year or the maximum time between events is in the interval of 5 to 10 years.

IV. **Unlikely** - if the crisis is anticipated to be a very rare event. Specifically, the frequency of occurrence is between 0.01 and 0.1 per year or the maximum time between events is in the range of 10 to 100 years.

V. **Very Unlikely** - if the crisis is considered an irrelevant or extremely rare threat. In this sense, the frequency of occurrence is below 0.01 per year or the maximum time between events is 100 years or more.

In relation to the **impact** of the crisis, two indicators are used to assess it, which are:

I. **EENS - Expected Energy Not Served.** This is the estimate of energy supplied and is expressed as a percentage of the annual energy demand.

II. **LOLE - Loss of Load Expectations.** This is the estimate of pressure drop and is expressed in hours

Taking into account these three variables (probability, EENS and LOLE) an assessment of the crisis scenarios is established, classifying them as *"Disaster", "Critical", "Important", "Minor"* or *"Insignificant"* and assigning the following assessment:

Crisis scenario rating	Value *(used for regional scenario rating)*
Disastrous	**10**
Critical	**5**
Major	**2**
Minor	**1**
Insignificant	**0**

In addition, the potential cross-border impact of the crises considered has been assessed. In the methodology a Cross-border Dependency Rating has been established. The assigned value depends on whether the crisis has no impact on other countries (value 1), whether the crisis may be susceptible to aggravating a crisis that is occurring simultaneously in at least one other country (value 1.2) or whether is liable to provoke a cross-border crisis due to direct or indirect causes in at least one other country (value 2)

Cross-border dependency rating	Value	Description
None	1	The crisis has no impact on other countries, even if they are facing simultaneous crisis.
Minor	1.2	The crisis is susceptible to aggravate a simultaneous crisis in at least one other country, either through direct or indirect causes (cf. Article 3).
Major	2	The crisis is susceptible to generate a cross-border crisis in at least one other country, either through direct or indirect causes (cf. Article 3).

This coefficient is used to correct the assessment obtained and thus obtain the final assessment of the scenarios for the corresponding Member States.

$$National\ Rating = Crisis\ Scenario\ Rating\ \times Cross\_border\ Dependency$$

Finally, as indicated in point 1.1, based on all the considerations related to probability, impact and transboundary effects, the 31 initial scenarios contemplated have been evaluated and, for Spain, 8 of the scenarios initially proposed by ENTSOe have been identified as those against which Spain should develop its corresponding National Risk-Preparedness Plan.

It should be noted that the Spanish Risk-Preparedness Plan has included a variation of the scenario corresponding to cyberattacks, which corresponds to a cyberattack on critical control, protection and telecommunications equipment (scenario E.3b) given that given that it has been deemed as feasible as scenario E.3a.

The results corresponding to the comprehensive evaluation and identification are shown below:

		Evaluación previa Escenarios Regionales ENTSOE					
Nº	Escenario	Likelihood	EENS (%) anual	LOLE (h)	Likelihood Impact	Cross-border	National Rating (0 -
E1	**Pandemia**	Possible	Insignificant	Minor	**Minor**	**Minor**	1,2
E2	**Tormenta extrema**	Possible	Insignificant	Minor	**Minor**	**Minor**	1,2
E3a	**Ciberataque a los Sistemas de Control**	Very unlikely	Disastrous	Major	**Minor**	**Major**	2
E3b	**Ciberataque a equipos críticos de control, protecciones y telecomunicaciones**	No incluido en los Escenarios Regionales ENTSOE					
E4	**Ataque físico a Centro Control**	Unlikely	Insignificant	Minor	**Insignificant**	**Minor**	0
E5	**Ataque físico a activos críticos**	Very unlikely	Disastrous	Disastrous	**Minor**	**Major**	2
E6	**Incendio o explosión en un activo crítico**	Unlikely	Minor	Insignificant	**Insignificant**	**Minor**	0
E7	**Sabotaje por parte de personal interno**	Possible	Insignificant	Insignificant	**Insignificant**	**None**	0
E8	**Incendio forestal**	Possible	Insignificant	Minor	**Minor**	**Minor**	1,2

2. Legal framework.

2.1 EU regulatory framework

2.1.1 Electricity sector

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.

As the regulation itself indicates in its preamble, *"[W]ell-functioning markets and systems, with adequate electricity interconnections, are the best guarantee of security of electricity supply. However, even where markets and systems function well and are interconnected, the risk of an electricity crisis, as a result of natural disasters, such as extreme weather conditions, malicious attacks or fuel shortages, can never be excluded."*

The European electricity market is made up by the electrical systems of the different Member States and even by the systems of other participants.

Taking into account that national electricity markets and systems are interconnected to a greater or lesser extent, the prevention and management of electricity crises should not be approached as exclusively national tasks.

Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 establishes a common approach and focus on the prevention and management of electricity crises, without forgetting that a common understanding is required between Member States.

The electricity crises contemplated in this regulation do not only affect a single member state, but, because of the previously mentinoed interconnections between systems, these crises can escalate and impact neighboring member states.

2.1.2 Oher regulation

CRITICAL INFRASTRUCTURES

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Modern states have a growing dependence on the complex infrastructure system that supports and enables the normal development of productive sectors, management and citizen life in general. This critical infrastructure system includeS, among others, some infrastructures of the electrical system and hence its relevance in the application of the National Risk-Preparedness in the Electricty Sector Plan.

This Directive establishes that the main and ultimate responsibility to protect European critical infrastructures falls upon the Member States and the infrastructure operators, and determines

the development of a series of obligations and actions by said States, which must be incorporated into national laws.

CYBERSECURITY

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems, establishes that Member States must guarantee the existence of an operational national contact point for the purposes of the information exchange on cyberattacks. Likewise, it establishes the need for them to have procedures so that, in the event of an urgent request for assistance, the competent authority can indicate, within a maximum period of eight hours from the receipt of the request for assistance, if it It may be attended, and the form and approximate term of it.

2.2 Spanish regulatory framework

2.2.1 Electricicity sector

Law 24/2013, of 26 December, of the Electricicty Sector.

The basic purpose of Law 24/2013, of 26 December, is to establish the regulation of the electricity sector, guaranteeing the electricity supply with the necessary levels of quality and at the lowest possible cost, ensuring the economic and financial sustainability of the system and allowing a level of effective competition in the electricity sector, all within the principles of environmental protection of a modern society.

Legal basis of the Plan in Spanish regulations

In the first place, it should be noted that the law includes a specific regulatory authorization relating to the guarantee of supply. In this sense, article 7 of Law 24/2013, of 26 December, establishes in section 2 that:

> *"2. The Government may adopt, for a specified period, the necessary measures to guarantee the supply of electrical energy when any of the following cases occur:*
>
> *a) Certain risk for the provision of electricity supply.*
>
> *b) Situations of shortage of one or more of the primary energy sources.*
>
> *c) Situations from which a serious threat to the physical integrity or safety of people, equipment or facilities or to the integrity of the electrical energy transmission or distribution network may be derived, prior notification to the affected Autonomous Communities.*
>
> *d) Situations in which there are substantial reductions in the availability of production, transport or distribution facilities or in the supply quality indices attributable to any of them. "*

In this way, the legal basis to act and prepare the necessary measures to face crises that threaten the electricity supply is established in the national regulations. Although these measures can be understood as very short-term measures that are carried out exclusively in response to events or situations that have already become apparent, it is unquestionable that they also include other types of measures such as the National Risk Preparedness in the Electricty Sector Plan itself.

Furthermore, article 7 itself establishes in section 3 that amogst these possible measures are *"any other measures that may be recommended by the international organizations of which Spain is a member or that are determined in application of those agreements in which it participates."*

The measures specifically provided for in section 3 of article 7 include all those derived from 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, including the National Risk-preparedness in the Electricity Sector Plan.

Analysis of the parties and activities related to crises in the electricity sector

Within the regulatory framework initially described, the aforementioned law defines the different activities for the supply of electrical energy, as well as the subjects who develop them. Among these subjects are some of which have special relevance in the context of the National Preparedness Plan for risks in the electricity sector and among which we can mention:

a) The system operator (SO), which is also the transport network manager (TSO).

b) The owner of the electricity transmission network (REE)

c) The distributors system operators (DSO)

d) Electricity generators

e) Consumers.

a) The system operator (SO/TSO)

In particular, it is worth highlighting the figure of the system operator, whose main function is to guarantee the continuity and security of the electricity supply and the correct coordination of the production and transport system. For this, and from a purely operational point of view, the system operator is enabled to:

i. Foresee and control the levels of electricity supply secutrity of the system in the short and medium term, both in the peninsular system and in the non-peninsular systems.

ii. Forecast in the short and medium term the demand for electrical energy, the use of production equipment

iii. Receive the necessary information on the maintenance plans of generation units, breakdowns or other circumstances.

Establish and control reliability measures of generation and transport network, affecting any element of the electrical system that is necessary, as well as the maneuvering plans for the replacement of the service in case of general failures in electricty supply, as well as coordinate and control its execution

iv. Give operating instructions of the transmission network, for its real-time operation

v. Determine the capacity to use international interconnections

vi. Provide all necessary instructions for the correct operation of the electrical system in accordance with reliability and safety criteria, and manage markets for system adjustment services that are necessary for this purpose.

Law 24/2013, of December 26, establishes that the system operator will be the TSO. To this end, in compliance with Directive 2009/72/EC of the European Parliament and the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC European Parliament and of the Council, of July 13, 2009, on common rules for the internal electricity market, and in particular, its article 10, the Government of Spain authorized and designated through Order IET/2209/2014, of 20 November, which authorizes and designates Red Electrica de España, S.A.U. TSO and thus SO.

It should be noted that, specifically in relation to risk-perparedness in the electricty sector, Law 24/2013, of December 26, expressly sets as a function of the system operator that it executes, within the scope of its functions, all those decisions that are adopted by the Government when:

a) There is a certain risk for electricity supply.

b) Situations of shortage of one or more of the primary energy sources occur.

c) Situations from which a serious threat to the physical integrity or safety of people, equipment or facilities or to the integrity of the electrical energy transmission or distribution network may arise, after notifying the affected Autonomous Communities.

d) Situations in which there are substantial reductions in generation, transport or distribution facilities or in whch the índices uesd to asses supply qualityare affected.

Thus, the basic regulatory framework sets up the actions of one of the main protagonists if a crisis occurs that risks partially or wholly electricity supply in Spain.

b) The transport network owner (REE)

Law 24/2013, of 26 December, also establishes the basic regulatory framework for the rest of the parties, agents or subjects that may have special relevance in the context of an electricity supply crisis and that were mentioned above: DSO, generators, consumers, etc.

That is why Law 24/2013, of 26 December, establishes that the trasnport network operator also is the owner of the transmission network and determines that it must be Red Eléctrica de España, S.A.

In relation to the plans to prepare for risks in the electricity sector, with regard to the activity of transporting electricity, the carrier has the following functions among its functions:

i. To carry out the instructions of the system operator that lead to restoring service in the event of general failures in the electrical power supply.

ii. To comply at all times with the instructions of the system operator for the operation of the transmission network, including international interconnections, for its maneuver in real time.

iii. To carry out, within the scope of his functions, those decisions that are adopted by the competent Public Administration in execution of the provisions of section 2 of article 7.

Regarding actions related to electricity crisis, the transport network owner will comply at all times with the instructions given by the system operator in the scope of his functions.

c) Dsitribution System Operators (DSO)

For its part, the electricity distribution is an activty that aims at the deliver electrical energy from the transmission network, or where appropriate from other distribution networks or from the generation connected to the distribution network itself, to consumers or other distribution networks in the required quality conditions with the ultimate aim of supplying it to consumers.

The parties that carry out this activity are the distirbution system operators and Law 24/2013, of 26 December, establishes that they have to:

i. Coordinate with adjacent DSO the maneuvering and maintenance actions carried out in the area of the networks they manage.

ii. Carry out the provisions or intructions of the system operator and TSO in the maneuvering plans for the restoration of service, in the event of general failures in the supply of electrical energy, controlling their execution and being able to affect any element of the distribution networks they manage.

iii. Provide the TSO and the adjacent DSO with sufficient information to guarantee a safe and efficient operation, coordinated development and interoperability of the interconnected network.

iv. Inform the competent public authorities and the subjects that could be affected, if any, of fraud and other anomalous situations

d) Electricity generators

Other relevant subjects in the electrical system and whose actions must be taken into consideration in crisis situations are the generators of electrical energy, which are those individuals or legal entities that have the function of generating electrical energy, as well as those of building, operating and maintain production facilities.

Among the regulated functions for the production activity and that may become relevant in the event of a crisis such as those contemplated in this plan, the following may be noted:

i. To carry out all those activities necessary to generate electricity in the terms provided in its authorization and, especially, with regard to safety, availability and maintenance of installed power and compliance with the environmental conditions required, without prejudice to the provisions for facilities for which a temporary closure has been authorized

ii. To connect and evacuate their energy through the transmission or distribution network according to the conditions that may be established by the system operator, where appropriate, the distribution network manager, for security reasons and those others that are established by regulation.

iii. To apply the measures that, in accordance with article 7 of this Law, are adopted by the Government

Although, traditionally, electricity generation had been characterized by plants connected to high voltage, the evolution towards distributed generation and self-consumption have promoted the appearance of smaller production facilities connected to lower voltages and closer to the centers. of consumption.

e) Consumers

Consumers, as they are considered in the sector, are the natural or legal persons who acquire energy for their own consumption and for the provision of energy recharging services for vehicles.

There is a great variety of consumers, ant their defining characteristic is the amount of energy that each one requires. Eletrictry demand continues to grow as electrical systems evolve with developments such as self-consumption, energy communities and other forms that promote the figures of prosumers and aggregators.

Finally, it should be noted that this basic framework has been developed by regulation in numerous norms and acts, some of which have special relevance in the operational actions for the operation of the electrical system and which are specified below.

Operating procedures

The operating procedures constitute a set of standards, of a technical and instrumental nature, necessary to carry out an adequate technical management of the peninsular electrical system and non-peninsular electrical systems.

These operating procedures are configured, therefore, as the way in which the subjects of the electrical system must specifically act, in particular in their day to day and even in the shorter term, including in those moments in which crises are occurring in the electricity sector.

Specifically, in relation to the response that the electrical system must give, as well as the subjects that participate in it, in the face of a power supply crisis, the following operating procedures should be highlighted, among others:

A. In the area of the Peninsular System, it is of special relevance:

i. **P.O. 6.1 Operational measures to guarantee coverage of demand in alert and emergency situations** - this procedure establishes the operational measures that the OS may adopt and that the affected agents must execute to guarantee coverage of demand in alert and emergency situations.

Other operating procedures related to the actions to be taken in response to electricity crises include:

ii. **P.O. 1.6 Establishment of security plans for the operation of the system -** this procedure defines the plans that must be established to guarantee the safe and reliable operation of the system and to carry out the restoration of service after severe incidents.

iii. **P.O. 2.2 Forecast of the coverage and safety analysis of the electrical system -** this procedure is intended to define the plans that must be established to guarantee the safe and reliable operation of the system and to carry out the restoration of service after severe incidents.

iv. **P.O. 3.2 Technical restrictions -** this procedure establishes the process for solving the technical restrictions identified in the Spanish peninsular electrical system in the Daily Base Operation Program (PDBF), as well as those that can be identified later during real-time operation.

v. **P.O. 3.3 Activation of balancing energies from the replacement reserve product (RR)** - the application in the Spanish peninsular electricity system of the European process of activation and exchange of balancing energies corresponding to the replacement reserve product, in accordance with the provisions of the Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation (SO Regulation) and Commission Regulation (EU) 2017/2195 of 23 November 2017 establishing a guideline on electricity balancing (EB Regulation).

vi. **P.O. 3.7 Application of limitations to energy production deliveries in non-resolvable situations with the application of system adjustment services -** this procedure establishes the system operation measures in such a way that the safe and stable operation of the system is maintained, in situations where the availability of power available for tertiary regulation is insufficient to ensure the proper balance between generation and consumption in the system or to solve risk situations in the system when the safety criteria established in the Operating Procedure are not met by which establishes the operating and safety criteria for the operation of the electrical system.

vii. **P.O. 4.0 Management of international connections -** this procedure establishes the way to manage the international interconnections of the Spanish mainland electricity system with France, Portugal, Morocco and Andorra.

viii. **P.O. 9.2 Exchange of information in real time with the system operator -** this procedure establishes the information in real time that the operator must exchange, the procedures and deadlines for exchanging information in real time and the system (OS) with the rest of the subjects of the peninsular electrical system for the fulfillment of their functions and obligations.

B. Similarly, in the area of Non-Peninsular Electricity Systems (SENP), the following are of special relevance:

i. **P.O. SENP 1 Operation of non-peninsular electrical systems -** this procedure establishes the safety and operation criteria that must be applied in the operation of non-peninsular Electrical Systems (SENP) and in the preparation and execution of safety plans, with the aim of guarantee the continuity of supply with the security and quality required.

ii. **P.O. SENP 2.2: Demand coverage, generation scheduling and additions to the economic dispatch -** this procedure encompasses the processes for the coverage of each of the SENP systems, in their annual, weekly, daily and intraday time horizons, in such a way that that it is possible to analyze the demand coverage of non-peninsular electrical systems, and schedule the necessary generation resources to achieve said coverage at the lowest possible cost, respecting safety and quality criteria.

iii. **P.O. SENP 3.1 Real-time generation scheduling -** this procedure is to establish the process for the resolution of deviations in real time between generation and consumption, as well as the resolution of technical restrictions that may appear in non-peninsular electrical systems.

iv. **P.O. SENP 9: information to be exchanged with the system operator -** this procedure defines the information to be exchanged by the system operator in order to perform the functions entrusted to it, as well as the form and deadlines in which it must be communicated or published, including the information related to their real-time situation, the information exchanged for the proper operation of the system and that required for the analysis of the SENP incidents.

Given the specificity, scale and territorial limitation of the electrical systems, it should be noted that, within their particularities, the same issues and matters are regulated as for the Peninsular System, although in a more concise manner. In some cases, the regulations that for the Peninsular System are included in several P.O. different.

2.2.2 Other regulation

CRITICAL INFRASTRUCTURES

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

In development of Council Directive 2008/114/EC of 8 December 2008, previosuly mentioned, Law 8/2011, of 28 April, was enacted.

Critical infrastructures, which are exposed to a series of threats, are among the most strategic national security priorities. For their protection, it is essential, on the one hand, to catalog the set of those that provide essential services to our society and, on the other, to design a plan that contains effective prevention and protection measures against possible threats to such infrastructures, both in the level of physical security as in that of the security of information and communication technologies.

As in the case of community regulations, the relevance of these regulations becomes clear when it is taken into account that the set of critical infrastructures includes, among others, some of the infrastructures corresponding to the national electricity system.

In the first place, as does Law 24/2013, of December 26, on the Electricity Sector for subjects of the electricity sector, this law establishes the basic regulatory framework for the State Security Forces and Bodies and other subjects in the framework of attacks carried out against infrastructures that are classified as critical.

In this sense, the security of critical infrastructures requires contemplating actions that go beyond the mere material protection against possible aggressions or attacks, which is why it is inevitable to involve other organs of the General State Administration, of the other Public Administrations, from other public bodies and the private sector. These critical infrastructures depend more and more on information technologies, both for their management and for their connection with other systems, for which they are mainly based on information and communication technologies of a public and open nature.

On the other hand, with regard to critical infrastructures in the energy sector and, specifically, in the electricity subsector, the Electric System Operator, the managers of the transmission networks play a relevant role in their protection and management. and electric power distribution and other agents in the sector, including electric power producers.

Also, Law 8/2011, of 28 April, establishes that the measures to be adopted in this matter are articulated in the following actions:

a) National Plan for the Protection of Critical Infrastructures.

b) Sectorial Strategic Plans.

c) Operator's Security Plans.

d) Specific Protection Plans.

e) Operational Support Plans.

Certain crisis scenarios included in the National Plan for Preparedness against Risks in the Electricity Sector are precisely cyberattacks or physical attacks on critical infrastructure in the electricity sector, and the preparation and response actions are specifically included and regulated in some of the plans. specifically mentioned in the previous paragraph. It should be noted that the aforementioned plans, as they apply to critical infrastructures and in accordance with the provisions of the regulations, are classified.

Royal Decree 704/2011, of 20 May, approving the Regulation for the protection of critical infrastructures.

This regulation develops, specifies and broadens the aspects contemplated in Law 8/2011, of 28 April. It articulates a complex interdepartmental system for the protection of critical infrastructures, composed of bodies and entities from both the Public Administrations and the private sector, nd it desings a comprehensive planning aimed at preventing and protecting the so-called critical infrastructures from threats or intentional acts originating from criminal figures such as terrorism, promoted through Communication technologies

Regarding the applicability and impact of this regulation in relation to any of the crisis scenarios of the electricity sector contemplated, it must be taken into account that this regulation adresses and includes special obligations that must be assumed by both the State and the operators of those Infrastructures that are determined as critical and that must be coordinated together with the actions aimed at guaranteeing the supply of electricity.

Specifically, this regulation establishes the specific regulation regarding the preparation and review of the aforementioned:

a) National Plan for the Protection of Critical Infrastructures.

b) Sectorial Strategic Plans.

c) Operator's Security Plans.

d) Specific Protection Plans.

e) Operational Support Plans.

National Plan for the Protection of Critical Infrastructures (PNPIC).

The Plan is an instrument whose basic objective is to keep safe the Spanish infrastructures that are considered critical. Critical infrastructures are those included in the National Catalog of Strategic Infrastructures and, conceptually, are those that provide a series of essential services to society. In this sense, part of the critical infrastructures include assets in the energy field.

The Plan includes a series of preventive and protective measures against certain threats that may affect critical infrastructures, be they of a physical nature or threats made through information and communication technologies.

Given the sensitive nature of the information contained therein, it is a classified document, registered in the National Center for the Protection of Critical Infrastructures (CNPIC), the first version of which was approved by the Secretary of State for Security in May 2007. The latest

revision of the PNPIC has been carried out through Instruction 01/2016 of February 10, of the Secretary of State for Security. Access to it is restricted to specifically authorized subjects.

CYBERSECURITY

Law 36/2015, of 28 September 28, on National Security.

National Security is understood as the action of the State aimed at protecting the freedom and well-being of its citizens, to guarantee the defense of Spain and its constitutional principles and values, as well as to contribute together with our partners and allies to international security in fulfillment of the commitments assumed; a concept that, to date, had not been the subject of comprehensive regulatory regulation.

Part of this Homeland Security concept includes cybersecurity. Specifically, the National Security Law considers cybersecurity as an area of special interest and that is why a boost is given to cybersecurity, which has modernized National Security, being one of the areas of greatest progress to date. Date

Royal Decree-Law 12/2018, of 7 September, on networks and information systems security.

The evolution of information and communication technologies, especially with the development of the Internet, has made information networks and systems play a crucial role in society, their reliability and security being essential aspects for the normal development of companies. economic and social activities.

This royal decree-law establishes a series of mechanisms that, with a comprehensive perspective, allow to improve protection against threats that affect information networks and systems, facilitating the coordination of actions carried out in this matter both at the level of national as well as with neighboring countries, in particular, within the European Union.

ICT services are right now and are becoming increasingly important in all energy sectors, including the electricity sector.

In relation to the above, it is configured as one of the competent authorities in cybersecurity for essential services operators and, regardless of the strategic sector in which such designation is made, the Secretary of State for Security, of the Ministry of the Interior, through the National Center for the Protection of Critical Infrastructures (CNPIC).

For its part, the Spanish National Cybersecurity Institute (INCIBE-CERT) is designated, among others, as the benchmark computer security incident response team in matters of network and information systems security.

Order PCI/487/2019, of 26 April, by which the 2019 National Cybersecurity Strategy is published, approved by the National Security Council.

The 2019 National Cybersecurity Strategy establishes Spain's position regarding a new concept of cybersecurity within the framework of the National Security Policy.

Cybersecurity extends beyond the field of merely protecting technological heritage into the political, economic and social spheres. In this sense, one of the most relevant areas in which it is applied is energy.

In addition to the actions to cause effects on digital systems, the conception of cyberspace as a vector of strategic communication must be taken into account, which can be used for the manipulation of information, disinformation campaigns or actions of a hybrid nature and to be protected.

3. Agents that take part in the National Risk-perparednesss in the Electricity Sector Plan. Competen Authority.

3.1 Introduction.

The National Risk-perparednesss in the Electricity Sector Plan requires the participation of a multiplicity of actors whose actions must lead to the best possible management of the identified electricity crises. The ultimate aim is electrictry supply security within the system.

The main agents involved in the actions derived from the plan are grouped into 3 main categories:

I. NATIONAL ELECTRICAL SYSTEM

The first of the pillars or blocks in which the National Risk-prepardeness in the Electrictry Sector Plan rests is that of the agents that directly belong to the Spanish electricity system and, in particaulr, the following must be taken into account:

- **Red Eléctrica de España, S.A.U.,** which is simultaneously the electricty System Operator, the TSO and the owner of the transport network.
- The different **Distribution System Operators (DSO)**
- **Generation companies**

As chapters 2, 3 and 4 of this plan establish, this agents have a direct and imnedaite participation in the management of supply crises. Their activity is direct and immediate and with the purpoe of operating the system during the crises so that the threats are either resolved or their impacts mitigated until they are finally solved. Their actions must ensure that the number of electricty supply incidents or interruptions are minimized.

II. PUBLIC AUTHORITIES

The second pillar is the one made up by the Public Sector. The most relevant agents which we can highlight are:

- **Government ministries and agencies**, such as**:**
    - **The Ministry for the Ecological Transition and the Demographic Challenge**, which is competent in energy matters and, in particular, the **Competent Authority** within the framework of the plan, as will be seen later.
    - **The Ministry of Health**, essential in the detection and actions associated with pandemics
    - **The Ministry of the Interior**, which is responsible for security matters. Those organizations, units and organizations that have a relevant role in the crisis scenarios contemplated in this plan are described below.

- **National Center for the Protection of Critical Infrastructures (CNPIC)**[3], a body belonging to the Ministry of the Interior, responsible for directing and coordinating the necessary actions to protect critical infrastructures, and the National Plan for the Protection of Critical Infrastructures.

- **National Institute of Cybersecurity of Spain (INCIBE)**[4] is a company dependent on the Ministry of Economic Affairs and Digital Transformation through the Secretary of State for Digitalization and Artificial Intelligence and consolidated as a reference entity for the development of cybersecurity and trust digital citizen, academic and research network, professionals, companies and especially for strategic sectors. INCIBE will be in charge of supporting the resolution of cyber incidents that may take place on the sector's infrastructures.

- **Cybersecurity Coordination Office (OCC)**[5], which is the technical coordinating body of the Secretary of State for Security in terms of cybersecurity and which also belongs to the Ministry of the Interior. Its functions, within the framework of this plan, include:

    - Provide a permanent early warning channel regarding vulnerabilities, cyberthreats and cyberattacks.

    - In the field of cybersecurity, establish information exchange channels between other actors, public and private, national and international.

    - Where appropriate, transfer the technical information of the incident to the State Security Forces and Bodies for investigation, if applicable.

As it will be seen throughout chapters 2, 3 and 4 of this plan, their participation in the management of supply crises in their áreas is direct and immediate and aimed at operating the crisis being resolved or mitigated until they are resolved, so that incidents in the electricity supply are minimized.

III. EMERGENCY AND OTHER FIRST RESPONSE SERVICES

The last pillar is the one configured by the Emergency and First Response Services[6]. Although their participation is not directly in the operation of the electrical system as either its subjects or agents, they are an element not only necessary but critical in the management of some, if not all, of the indentified scenarios. This category includes:

- **The National Police Force,**

- **The Civil Guard**

- **The police forces of the different autonomous communities**

- **Civil Protection services**

[3] Centro Nacional de Protección de Infraestructuras Críticas (CNPIC)
[4] Instituto Nacional de Ciberseguridad de España (INCIBE)
[5] Oficina de Coordinación de Ciberseguridad (OCC)
[6] The National Police Force, the police forces of the diferente autonomous communities and the Civil Guard are collectively known as “Fuerzas y Cuerpos de Seguridad del Estado” (FCSE)

- **Firefighters**
- **Medical Emergency Services and Red Cross**
- **Emergency Military Unit (UME)**[7]

[7] Unidad Militar de Emergencias (UME)

3.2 Competent Authority.

As notified to the European Commission in March 2020, the competent authority responsible for carrying out the tasks contained in Regulation (EU) 2019/941 of the European Parliament and of the Council of June 5, 2019 is the Ministry for the Ecological Transition and the Demographic Challenge.

As established in section 2 of article 3 of the aforementioned Regulation, within the competent authority, the following are the contact persons for the purposes thereof:

i. **General Director of Energy Policy and Mines**

ii. **General Deputy Director of Electric Energy.**

3.2.1 Functions and responsibilities.

In accordance with Article 3 of Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019, the Ministry for the Ecological Transition and the Demographic Challenge will be responsible for carrying out the different tasks provided for in the Regulations, which include, among others:

- Prepare and review the national risk-preparedness in the electrictry sector plans.
- Cooperate with the Competent Authorities from other Member States in electricity sector crises when there is a possibility that they may have cross-border impacts.
- Inform Member States and the European Commission of the threats and risks detected in Spain of potential electricity supply crises, even when it is not foreseeable that it will have cross-border repercusions. These communications will preferably be made through the Electricity Coordination Group (ECG) of the European Commission.
- Issue early warnings to the European Commission, to the Competent Authorities of the Member States in the same region and, if they do not belong to this region, to the competent authorities of the directly connected Member States. The information accompanying these alerts will include, when possible:
    - Information on the causes of the possible electricity crisis.
    - What measures are taken or planned to prevent an electricity crisis from occurring.
    - What are the chances that assistance from other Member States will be needed.
- When faced with an electricity crisis, after consulting the transmission grid manager, declare the crisis and inform the competent authorities of the Member States of the same region and, if they do not belong to this region, the authorities. competent authorities of the directly connected Member States, as well as the Commission.
- When an electricity crisis occurs, submit the ex post evaluation reports to the Electricity Coordination Group and the Commission, after consulting the regulatory authority. For this, it may request the collaboration of the System Operator in the preparation of the evaluation report or delegate the same to the same.

Along with those established by law, the following will be the responsibility of the Competent Authority:

- Communicate to the citizens on the evolution of the crisis and the measures that are prepared, in place or have already been taken.
- Coordinate with the rest of the Government and Administration bodies in order to help each body carry out all the necessary functions, roles and competences that they have in order to help solve the electrictry supplu crises.
- Push thorugh necessary legislation/regulation in order to solve elecrtictry supply crises.

3.2.2 Delegated functions.

None of the functions provided for the competent authority in Regulation (EU) 2019/941 of the European Parliament and of the Council of June 5, 2019, have been delegated to other entities, all without prejudice to possible future delegations in accordance with the point 3 of article 3 of Regulation (EU) 941/2019 of the European Parliament and of the Council of 5 June 5 2019, which in any case would be reflected in successive updates of this Plan.

4. Procedures and actions.

The 8 National Electricity Crisis Scenarios and their variants contemplated for the National Preparedness Plan are those that have been identified in Chapter 1 of this plan and are summarized below:

1. Pandemic
2. Extreme storm
3. Cyberattack:
    i. Cyberattack to Control Systems
    ii. Cyberattack to critical control, protection and/or telecommunications equipment
4. Physical attack on Control Center
5. Physical attack on critical assets
6. Fire or explosion at a critical asset
7. Insider sabotage
8. Forest fire

Once the scearnios have been properly identified in Chapter 1, this chapter proceeds to describe them in detail. This description includes in detail the specific plans, procedures and actions for each of the scenarios using the following structure:

I. I. Initiating event of the crisis:

a. Crisis Detection

b. Agents involved.

II. II. Description of the measures to be adopted:

a. At national level:

i. Preventive measures, which must have been taken before the crisis

ii. Measures taken to respond to or mitigate the crisis

b. At regional or bilateral level:

i. Preventive measures, which must have been taken before the crisis

ii. Measures taken to respond to or mitigate the crisis

III. Impact

IV. Ex-post evaluation and improvement actions.

4.1 Pandemic.

Pandemics are international by nature and their initiating event, if it can be classified as such, is that a certain number of nationally confirmed cases is reached. The determination of a contagious outbreak as a pandemic is done by the Ministry of Health or, where appropriate, the Presidency of the Government.

In order for a pandemic to be considered as a electrictry sector crisis, it is not in essence necessary that a certain number of confirmed cases must be reached within the electricity sector itself, but rather that from a fundamentally practical point of view the measures are adopted in sufficnete anticipation, always with the objective of minimizing or even preventing the negative impact of the pandemic.

The main incidents of a pandemic in the electricity sector are precisely derived from the number of confirmed cases within the electricity sector and, in particular, in the System Operator, in the TSO and DSOs and in the personnel of the system control centers, among others.

These confirmed cases can lead to a significant reduction in available workforce and they can have a cascading effect on suppliers and contractors, as well as downstream consumers.

The impacts that can foreseeably occur as a result of this type of crisis are in essence two:

- There are fewer resources that can solve incidents at checkpoints.
- There is an greater probability of an electrical crisis taking place if, in the event of a fortuitous failure in a critical system or a critical network element, its resolution is delayed due to lack of personnel and results in a multiple failure

When considering cross-border impacts for this type of crisis, it is most likely that other Member States (including those in the region in which Spain is included) will be in idenitcal or a very similar situation.

The most recent examples of this type of crises include the Influenza A pandemic in 2009 and, more recently, Covid-19 pandemic.

The main characteristics of this crisis scenario and the actions that are to be taken in it are describe below:

I. CRISIS TRIGGER EVENT
Crisis Detection
Communication through official bodies, which, as indicated above, include the Ministry of Health and, where appropriate, the Presidency of the Government.
Agents involved
The following agents involved have been identified: Red Eléctrica de España, S.A., the Distribution System Operators (DSO), Generation Companies, State Security Forces and Bodies (FCSE), Official Bodies.
II. MEASURES TO BE ADOPTED DURING THE CRISIS

Preventive measures at national level

Steps that can be taken before the crisis include:

- Isolate Control Centers: reorganize work shifts, avoiding contact between the different Control Centers and between the different shifts.
- Limit the physical presence of staff.
- Increase cleaning and disinfection measures.
- Give the necessary prioritization to operation tasks and field work.
- Strengthen coordination between the different agents: establis different scenarios and, accordingly, reassign tasks

Mitigating or response measures at national level

Actions to be taken during the crisis include the following:

a) Measures related to the operation of the system:

- Depending on the electricity supply crisis that may occur, the System Operator will carry out the measures included in the Operating Procedures for the different emergency states of the system (alert, emergency, replacement).
- Additional measures for voltage control due to the different possible demand scenarios.

b) Other measures: not considered

Preventive measures at regional level

There are no preventive measures at the regional level for this type of electricity system crisis scenarios.

Mitigating or response measures at regional level

Measures that can be taken during the crisis, when it has cross-border impact, include the following:

- Carry out active power support exchanges with neighboring TSOs
- Support procedure of the Spanish and French systems for the restoration of service after generalized incidents
- Support procedure of the Spanish and Portuguese systems for the restoration of the service after generalized incidents

III. IMPACT

The crisis is expected to have an impact on consumers, Distribution System Operators (DSO), Generators, as well as, in the case of a regional crisis, in neighboring TSOs.

IV. EX-POST EVALUATION AND IMPROVEMENT ACTIONS

In this regard, actions to be taken include:

- Carry out analysis and correlation of events to reconstruct the sequence of events.
- Preapre report, which includes lessons learned and improvement actions

- Participate in international work groups for the analysis of incidents (eg. European Network of Transport System Operators (ENTSOe))

4.2 Extreme storm.

Storms are natural weather phenomena. Taking into account the geography of Spain and the Iberian Peninsula, not only cannot significant impacts at the regional level be ruled out, but they are predictable.

The initiating event in this type of crises in the electricity sector is a strong wind and snow storm. As such, it is foreseeable that this event could lead to a significant loss of supply and that it is characterized by a drop in supports, affecting other elements of the electrical system.

Within this crisis scenario, the accumulation of snow is expected to hinder access for repairs.

The impacts that can foreseeably occur as a consequence of this type of crises are esentially:

- Physical or operational damage to elements of the electrical system.
- Market outages take place.
- That the fiber optic cables are affected.
- That there is a loss of remote control in the operation of the electrical system.

When analysing cross-border impacts for this type of crisis, it is foreseeable that the storm could also affect countries in Western Europe. In this sense, a possible loss of interconnection lines is assumed and, therefore, a potential reduction in exchange capacity with France and Portugal.

The most recent references to this type of crises include Cyclone Klaus (2009) and Temporal Gloria (2020).

The main characteristics of this crisis scenario and the actions that are to be taken in it are describe below:

I. CRISIS TRIGGER EVENT CRISIS
Crisis Detection
Weather information or alerts.
Agents involved
The following agents involved have been identified: Red Eléctrica de España, S.A., the Distribution System Operators (DSO), Generation Companies, State Security Forces and Bodies (FCSE), Official Bodies (National Center for the Protection of Critical Infrastructures (CNPIC), Ministries), Emergency Military Unit (UME)
II. MEASURES TO BE ADOPTED DURING THE CRISIS
Preventive measures at national level

Steps that can be taken before the crisis include:

- Coupling of lines to increase the network mesh level and avoid the formation of ice sleeves on uncoupled lines
- Assess the return of discharges and the replacement of elements
- Manage existing generation reserves (Coupling groups, management of group unavailability)
- Implement the cancellation of line/unit reclosures, allocation of field personnel to identify affected lines and open lines.

Mitigating or response measures at national level

Actions to be taken during the crisis include the following:

a) System Operation Measures:

- Application of technical restrictions in real time to manage frequency deviations outside the established limits
- Generation management through generation redispatches
- Adaptation of exchange programs with France, Portugal, Andorra and Morocco
- In the event of remote control loss, allocation of field personnel to critical Electrical Substations and dispatch of instructions and communication with agents via telephone.
- Additional measures for voltage control depending on the different demand scenarios
- Return of discharges
- Manual load shedding
- Automatic load shedding by underfrequency mechanisms and schemes: it includes the disconnection of pumping groups and later preselected load shedding
- Automatic overfrequency control mechanisms and schemes: includes automatic generation disconnection plan

b) Other measures:

The application of protocols includes different scenarios in the event of the impossibility or limitation of mobility, where the following are contemplated: shift organization, accommodation, supplies and facilities

Preventive measure at regional level

Carry out the adaptation of exchange programs with neighboring Member States, as well as with neighboring third countries.

Mitigating or response measures at regional level

Measures that can be taken during the crisis, when it has cross-border impact, include the following:

- Carry out active power support exchanges with neighboring TSOs
- Support procedure of the Spanish and French systems for the restoration of service after generalized incidents
- Support procedure of the Spanish and Portuguese systems for the restoration of the service after generalized incidents.

III. IMPACT

The crisis is expected to have an impact on consumers, Distribution System Operators (DSO), Generators, as well as, in the case of a regional crisis, in neighboring TSOs.

IV. EX-POST EVALUATION AND IMPROVEMENT

In this regard, actions to be taken include:

- Carry out analysis and correlation of events to reconstruct the sequence of events.
- Preapre report, which includes lessons learned and improvement actions
- Participate in international work groups for the analysis of incidents (eg. European Network of Transport System Operators (ENTSOe))

4.3 Cyberattack to Control Systems.

Cyber attacks are intentional incidents. Taking into account their seriousness and objectives, not only cannot marked impacts at the regional level be ruled out, but their transboundary impact are rather a strong possibility.

In this scenario, the initiating event in this type of crisis in the electricity sector is a cyberattack on the Control Systems (either the main one, the emergency or, more predictably, both) and the remote units. This attack would manifest itself in a denial of service, in illegal access attempts or in the manipulation of the information used by the control systems. Ultimately, this would lead to problems in the operation of the system.

The impacts that can foreseeably occur as a consequence of this type of crisis are fundamentally:

- Unforeseen lines open.
- Unplanned or unforeseen trips take place in the generation units.
- That there is an operating loss in the electricity market.

Regarding the cross-border impact of this type of crisis, it is considered plausible that a cyber attack on control systems, depending on its severity, could also affect our neighboring countries. This cross-border impact would manifest itself in a possible loss of the international interconnections that Spain has with France and Portugal.

At present there is no reference for this type of crisis.

The main characteristics of this crisis scenario and the actions that are to be taken in it are describe below:

I. CRISIS TRIGGER EVENT
Crisis Detection
Security Operations Centers (SOC) of Red Eléctrica de España, S.A.U.
Agents involved
The following agents involved have been identified: Red Eléctrica de España, S.A., the Distribution System Operators (DSO), Generation Companies, State Security Forces and Bodies (FCSE), Official Bodies (National Center for the Protection of Critical Infrastructures (CNPIC), National Institute of Cybersecurity of Spain (INCIBE), Cybersecurity Coordination Office (OCC), Ministries).
II. MEASURES TO BE ADOPTED DURING THE CRISIS
Preventive measures at national level

Steps that can be taken before the crisis include:

- Carry out potential risk analysis
- Establish a Planning and apply it
- Perform monitoring of accesses and systems
- Secure development of operational applications
- Carry out the implementation of anti-intrusion measures and controls
- Control access of people and vehicles (includes authentication)
- Safe installation and configuration of malware protection
- Apply and review privilege management
- Have back up elements
- Have an active redundant Control Center

Mitigating or response measures at national level

Actions to be taken during the crisis include the following:

a) System Operation Measures:

- Application of technical restrictions in real time to manage frequency deviations outside the established limits
- Generation management through generation redispatches
- Adaptation of exchange programs with France, Portugal, Andorra and Morocco
- In the event of remote control loss, allocation of field personnel to critical Electrical Substations and dispatch of instructions and communication with agents via telephone.
- Additional measures for voltage control depending on the different demand scenarios
- Return of discharges
- Manual load shedding
- Automatic load shedding by underfrequency mechanisms and schemes: it includes the disconnection of pumping groups and later preselected load shedding
- Automatic overfrequency control mechanisms and schemes: includes automatic generation disconnection plan

b) Other measures:

- Proceed to the Declaration of Applicability.
- Communication with the OCC and the Security Incident Response Center for citizens and companies is renamed INCIBE-CERT of reference.
- Application of the Continuity Plan in the event of unavailability of technological assets.

Preventive meausres at regional level

There are no preventive measures at the regional level for this type of electricity system crisis scenarios.

Mitigating or response measures at regional level

Measures that can be taken during the crisis, when it has cross-border impact, include the following:

- Carry out active power support exchanges with neighboring TSOs
- Support procedure of the Spanish and French systems for the restoration of service after generalized incidents
- Support procedure of the Spanish and Portuguese systems for the restoration of the service after generalized incidents

III. IMPACT

The crisis is expected to have an impact on consumers, Distribution System Operators (DSO), Generators, as well as, in the case of a regional crisis, in neighboring TSOs.

IV. EX-POST EVALUATION AND IMPROVEMENT

In this regard, actions to be taken include:

- Carry out analysis and correlation of events to reconstruct the sequence of events.
- Preapre report, which includes lessons learned and improvement actions
- Participate in international work groups for the analysis of incidents (eg. European Network of Transport System Operators (ENTSOe))

4.4 Cyberattack to critical control, proteciton and/or telecommunictions equipment.

As mentioned in the previous scenario, cyberattacks are intentional incidents. Taking into account their seriousness and objectives, not only cannot marked impacts at the regional level be ruled out, but their transboundary impact is rather possible.

In this scenario, the initiating event in this type of crisis in the electricity sector is a cyberattack on critical control, protection and telecommunications equipment. This attack would manifest itself in a denial of service, in illegal access attempts or in the manipulation of the information used by the control systems. Ultimately, this would lead to problems in the operation of the system.

The impacts that are most likely to occur as a consequence of this type of crisis are fundamentally:

- Multiple simultaneous position trips occur in several critical substations.
- That unplanned or foreseen trips take place in the generation units.
- That there is an operating loss in the electricity market.

With regard to the cross-border impact of this type of crisis, it is considered probable that a cyberattack on control systems, taking into account its severity and magnitude, could also affect our neighboring countries. This cross-border impact would manifest itself in a possible loss of the interconnection lines that Spain has with France and Portugal.

The most recent reference to this type of crisis is the cyberattack on the electricity grid in Ukraine (2015).

The main characteristics of this crisis scenario and the actions that are to be taken in it are describe below:

I. CRISIS TRIGGER EVENT CRISIS
Crisis Detection
Security Operations Centers (SOC) of Red Eléctrica de España, S.A.U.
Agents involved
The following agents involved have been identified: Red Eléctrica de España, S.A., the Distribution System Operators (DSO), Generation Companies, State Security Forces and Bodies (FCSE), Official Bodies (National Center for the Protection of Critical Infrastructures (CNPIC), National Institute of Cybersecurity of Spain (INCIBE), Cybersecurity Coordination Office (OCC), Ministries).
II. MEASURES TO BE ADOPTED DURING THE CRISIS
Preventive measures at national level

Steps that can be taken before the crisis include:

- Carry out physical and electronic perimeter security
- Establish and apply job protection measures
- Carry out access control for people and vehicles (including authentication) to the critical assets in question.
- Carry out user registers of control centers
- Apply and review privilege management
- Have back up elements
- Have an active redundant Control Center

Mitigating or response measures at national level

Actions to be taken during the crisis include the following:

a) System Operation Measures:

- Application of technical restrictions in real time to manage frequency deviations outside the established limits
- Generation management through generation redispatches
- Adaptation of exchange programs with France, Portugal, Andorra and Morocco
- In the event of remote control loss, allocation of field personnel to critical Electrical Substations and dispatch of instructions and communication with agents via telephone.
- Additional measures for voltage control depending on the different demand scenarios
- Return of discharges
- Manual load shedding
- Automatic load shedding by underfrequency mechanisms and schemes: it includes the disconnection of pumping groups and later preselected load shedding
- Automatic overfrequency control mechanisms and schemes: includes automatic generation disconnection plan

b) Other measures:

- Proceed to the Declaration of Applicability.
- Communication with the OCC and the Security Incident Response Center for citizens and companies is renamed INCIBE-CERT of reference.
- Application of the Continuity Plan in the event of unavailability of technological assets.

Preventive meausres at regional level

There are no preventive measures at the regional level for this type of electricity system crisis scenarios.

Mitigating or response measures at regional level

Measures that can be taken during the crisis, when it has cross-border impact, include the following:

- Carry out active power support exchanges with neighboring TSOs
- Support procedure of the Spanish and French systems for the restoration of service after generalized incidents
- Support procedure of the Spanish and Portuguese systems for the restoration of the service after generalized incidents

III. IMPACT

The crisis is expected to have an impact on consumers, Distribution System Operators (DSO), Generators, as well as, in the case of a regional crisis, in neighboring TSOs.

IV. EX-POST EVALUATION AND IMPROVEMENT

In this regard, actions to be taken include:

- Carry out analysis and correlation of events to reconstruct the sequence of events.
- Preapre report, which includes lessons learned and improvement actions
- Participate in international work groups for the analysis of incidents (eg. European Network of Transport System Operators (ENTSOe))

4.5 Physical attack on Control Center.

Physical attacks on facilities and infrastructure are intentional incidents. Taking into account their seriousness and objectives, not only cannot marked impacts at the regional level be ruled out, but their transboundary impact is alos rather possible.

In this scenario, the initiating event in this type of crisis in the electricity sector is a physical attack on a Main Control Center, a Back-up Control Center or simultaneously on centers of both types.

The impacts that are most likely to occur as a result of this type of attack are fundamentally:

- That there is an impossibility to operate the assets of the affected Control Center
- That there is an operating loss in the electricity market.
- That a partial or total blackout occurs

Regarding the cross-border impact of this type of crisis, it is considered probable that a physical attack on one or more Control Centers (if coordinated) could also affect our neighboring countries. This cross-border impact would manifest itself in a possible loss of synchronism within continental Europe electrictry system.

At present there is no reference for this type of crisis.

The main characteristics of this crisis scenario and the actions that are to be taken in it are describe below:

I. CRISIS TRIGGER EVENT CRISIS
Crisis Detection
Physical Security Unit of Red Eléctrica de España, S.A.U.
Agents involved
The following agents involved have been identified: Red Eléctrica de España, S.A., the Distribution System Operators (DSO), Generation Companies, State Security Forces and Bodies (FCSE), Official Bodies (National Center for the Protection of Critical Infrastructures (CNPIC), National Institute of Cybersecurity of Spain (INCIBE), Cybersecurity Coordination Office (OCC), Ministries).
II. MEASURES TO BE ADOPTED DURING THE CRISIS
Preventive measures at national level
Steps that can be taken before the crisis include: • Carry out physical and electronic perimeter security • Establish and apply job protection measures • Carry out access control for people and vehicles (including authentication) to the critical assets in question. • Carry out user registers of control centers • Apply and review privilege management

- Have back up elements
- Have an active redundant Control Center

Mitigating or response measures at national level

Actions to be taken during the crisis include the following:

a) System Operation Measures:

- Application of technical restrictions in real time to manage frequency deviations outside the established limits
- Generation management through generation redispatches
- Adaptation of exchange programs with France, Portugal, Andorra and Morocco
- In the event of remote control loss, allocation of field personnel to critical Electrical Substations and dispatch of instructions and communication with agents via telephone.
- Additional measures for voltage control depending on the different demand scenarios
- Return of discharges
- Manual load shedding
- Automatic load shedding by underfrequency mechanisms and schemes: it includes the disconnection of pumping groups and later preselected load shedding
- Automatic overfrequency control mechanisms and schemes: includes automatic generation disconnection plan

b) Other measures:

- Activation of the SES-OCC-FCSE Communications Protocol (Secretary of State for Security - Cybersecurity Coordination Office - State Security Forces and Bodies)
- Activation, where appropriate, of the operator's safety plans. The Interlocutor with whom communications will be maintained within the scope of this plan is the National Center for the Protection of Critical Infrastructures (CNPIC).
- Activation of Specific Protection Plans. The Interlocutor with whom communications will be maintained within the scope of this plan is the CNPIC and there will also be communications with the State Security Forces (FCSE)
- Activation of the Operational Support Plans. The deployment actions will be carried out by the FCSE

Preventive meausres at regional level

There are no preventive measures at the regional level for this type of electricity system crisis scenarios.

Mitigating or response measures at regional level

Measures that can be taken during the crisis, when it has cross-border impact, include the following:

- Carry out active power support exchanges with neighboring TSOs
- Support procedure of the Spanish and French systems for the restoration of service after generalized incidents
- Support procedure of the Spanish and Portuguese systems for the restoration of the service after generalized incidents

III. IMPACT

The crisis is expected to have an impact on consumers, Distribution System Operators (DSO), Generators, as well as, in the case of a regional crisis, in neighboring TSOs.

IV. EX-POST EVALUATION AND IMPROVEMENT

In this regard, actions to be taken include:

- Carry out analysis and correlation of events to reconstruct the sequence of events.
- Preapre report, which includes lessons learned and improvement actions
- Participate in international work groups for the analysis of incidents (eg. European Network of Transport System Operators (ENTSOe))

4.6 Physical attack on critical assets.

As previously commented for physical attacks on one or more Control Centers, physical attacks on facilities and infrastructures are intentional incidents. Taking into account their seriousness and objectives, not only cannot marked impacts at the regional level be ruled out, but their transboundary impact are possible.

The National Inventory of National Critical Assets (INACN)[8] is the registry that contains complete and updated information on the National Critical Assets located in the Spanish territory. As mentioned, this list includes some assets in the electricity sector.

In this scenario, the initiating event in this type of crisis in the electricity sector is a physical attack on one or more critical assets, including substations, lines, generation groups, data centers, etc.

The impacts that are most likely to occur as a consequence of this type of crisis are fundamentally:

- Damage to critical assets
- That there is an operating loss in the local electricity market.

Regarding the cross-border impact of this type of crisis, it is considered probable that a physical attack on one or more critical assets (if coordinated) could also affect our neighboring countries. This cross-border impact would manifest itself not only in a loss of interconnection lines, but also a loss of synchronism with the European Continental System could occur if the attack affects the entire Spain-France interconnection.

At present there is no reference for this type of crises in the European Union.

The main characteristics of this crisis scenario and the actions that are to be taken in it are describe below:

I. CRISIS TRIGGER EVENT CRISIS
Crisis Detection
Physical Security Unit of Red Eléctrica de España, S.A.U.
Agents involved
The following agents involved have been identified: Red Eléctrica de España, S.A., the Distribution System Operators (DSO), Generation Companies, State Security Forces and Bodies (FCSE), Official Bodies (National Center for the Protection of Critical Infrastructures (CNPIC), National Institute of Cybersecurity of Spain (INCIBE), Cybersecurity Coordination Office (OCC), Ministries).
II. MEASURES TO BE ADOPTED DURING THE CRISIS
Preventive measures at national level

[8] Inventario Nacional de los Activos Críticos Nacionales (INACN)

Steps that can be taken before the crisis include:

- Carry out physical and electronic perimeter security
- Establish and apply job protection measures
- Carry out access control for people and vehicles (including authentication) to the critical assets in question.
- Carry out user registers of control centers
- Apply and review privilege management
- Have back up elements
- Have an active redundant Control Center

Mitigating or response measures at national level

Actions to be taken during the crisis include the following:

a) System Operation Measures:

- Application of technical restrictions in real time to manage frequency deviations outside the established limits
- Generation management through generation redispatches
- Adaptation of exchange programs with France, Portugal, Andorra and Morocco
- In the event of remote control loss, allocation of field personnel to critical Electrical Substations and dispatch of instructions and communication with agents via telephone.
- Additional measures for voltage control depending on the different demand scenarios
- Return of discharges
- Manual load shedding
- Automatic load shedding by underfrequency mechanisms and schemes: it includes the disconnection of pumping groups and later preselected load shedding
- Automatic overfrequency control mechanisms and schemes: includes automatic generation disconnection plan

b) Other measures:

- Activation of the SES-OCC-FCSE Communications Protocol (Secretary of State for Security - Cybersecurity Coordination Office - State Security Forces and Bodies)
- Activation, where appropriate, of the operator's safety plans. The Interlocutor with whom communications will be maintained within the scope of this plan is the National Center for the Protection of Critical Infrastructures (CNPIC).
- Activation of Specific Protection Plans. The Interlocutor with whom communications will be maintained within the scope of this plan is the CNPIC and there will also be communications with the State Security Forces (FCSE)
- Activation of the Operational Support Plans. The deployment actions will be carried out by the FCSE

Preventive meausres at regional level

There are no preventive measures at the regional level for this type of electricity system crisis scenarios.

Mitigating or response measures at regional level
Measures that can be taken during the crisis, when it has cross-border impact, include the following: • Carry out active power support exchanges with neighboring TSOs • Support procedure of the Spanish and French systems for the restoration of service after generalized incidents • Support procedure of the Spanish and Portuguese systems for the restoration of the service after generalized incidents
III. IMPACT
The crisis is expected to have an impact on consumers, Distribution System Operators (DSO), Generators, as well as, in the case of a regional crisis, in neighboring TSOs.
IV. EX-POST EVALUATION AND IMPROVEMENT
In this regard, actions to be taken include: • Carry out analysis and correlation of events to reconstruct the sequence of events. • Preapre report, which includes lessons learned and improvement actions • Participate in international work groups for the analysis of incidents (eg. European Network of Transport System Operators (ENTSOe))

4.7 Fire or explosión at a critical asset.

Unlike crises caused by physical attacks, scenarios of fires or explosions in assets, facilities and infrastructures are considered as situations in which the incident is unintentional. However, as in the cases of deliberate attacks and taking into account their severity and objectives, not only cannot marked impacts at the regional level be ruled out, but their transboundary impact is also rather possible.

In this scenario, the initiating event in this type of power sector crisis is an unintended fire or explosion at a critical asset. The impacts that are most likely to occur as a result of this type of incident are fundamentally:

- Damage to critical assets
- That there is an operating loss in the local electricity market.

Regarding the cross-border impact of this type of crisis, it is considered probable that an incident in which an incident or explosion takes place in one of the critical assets could also affect our neighboring countries. This cross-border impact would fundamentally manifest itself in losses of the interconnection lines, if these are the assets that have suffered the fire or explosion or are close to said assets or are connected to them.

At present there is no reference for this type of crises in the European Union.

The main characteristics of this crisis scenario and the actions that are to be taken in it are describe below:

I. CRISIS TRIGGER EVENT CRISIS
Crisis Detection
Physical Security Unit of Red Eléctrica de España, S.A.U.
Agents involved
The following agents involved have been identified: Red Eléctrica de España, S.A., the Distribution System Operators (DSO), Generation Companies, State Security Forces and Bodies (FCSE), Official Bodies (National Center for the Protection of Critical Infrastructures (CNPIC), National Institute of Cybersecurity of Spain (INCIBE), Cybersecurity Coordination Office (OCC), Ministries).
II. MEASURES TO BE ADOPTED DURING THE CRISIS
Preventive measures at national level
Steps that can be taken before the crisis include: • Have back up elements • Have an active redundant Control Center

Mitigating or response measures at national level

Actions to be taken during the crisis include the following:

a) System Operation Measures:

- Application of technical restrictions in real time to manage frequency deviations outside the established limits
- Generation management through generation redispatches
- Adaptation of exchange programs with France, Portugal, Andorra and Morocco
- In the event of remote control loss, allocation of field personnel to critical Electrical Substations and dispatch of instructions and communication with agents via telephone.
- Additional measures for voltage control depending on the different demand scenarios
- Return of discharges
- Manual load shedding
- Automatic load shedding by underfrequency mechanisms and schemes: it includes the disconnection of pumping groups and later preselected load shedding
- Automatic overfrequency control mechanisms and schemes: includes automatic generation disconnection plan

b) Other measures:

- Activation of the SES-OCC-FCSE Communications Protocol (Secretary of State for Security - Cybersecurity Coordination Office - State Security Forces and Bodies)
- Activation, where appropriate, of the operator's safety plans. The Interlocutor with whom communications will be maintained within the scope of this plan is the National Center for the Protection of Critical Infrastructures (CNPIC).
- Activation of Specific Protection Plans. The Interlocutor with whom communications will be maintained within the scope of this plan is the CNPIC and there will also be communications with the State Security Forces (FCSE)
- Activation of the Operational Support Plans. The deployment actions will be carried out by the FCSE

Preventive meausres at regional level

There are no preventive measures at the regional level for this type of electricity system crisis scenarios.

Mitigating or response measures at regional level

Measures that can be taken during the crisis, when it has cross-border impact, include the following:

- Carry out active power support exchanges with neighboring TSOs
- Support procedure of the Spanish and French systems for the restoration of service after generalized incidents
- Support procedure of the Spanish and Portuguese systems for the restoration of the service after generalized incidents

III. IMPACT

The crisis is expected to have an impact on consumers, Distribution System Operators (DSO), Generators, as well as, in the case of a regional crisis, in neighboring TSOs.

IV. EX-POST EVALUATION AND IMPROVEMENT

In this regard, actions to be taken include:

- Carry out analysis and correlation of events to reconstruct the sequence of events.
- Preapre report, which includes lessons learned and improvement actions
- Participate in international work groups for the analysis of incidents (eg. European Network of Transport System Operators (ENTSOe))

4.8 Insider sabotage.

As commented for physical attacks on one or more Control Centers or physical attacks on critical assets, sabotages by internal personnel are intentional incidents. Taking into account their seriousness and objectives, not only cannot marked impacts at the regional level be ruled out, but rather their transboundary impact is possible.

In this scenario, the initiating event in this type of crisis in the electricity sector is an intentional manipulation of critical systems by internal personnel under threat or bribery.

The impacts that are most likely to occur as a consequence of this type of crisis are fundamentally:

- That the multiple opening of elements of the electrical energy transmission or distribution network takes place
- Generation group shots being fired.

Regarding the cross-border impact of this type of crisis, it is considered probable that a physical attack on one or more critical assets (if coordinated) could also affect our neighboring countries. This cross-border impact would fundamentally manifest itself in losses of the interconnection lines, if these are the assets that have suffered the incident.

At present there is no reference for this type of crises in the European Union.

The main characteristics of this crisis scenario and the actions that are to be taken in it are describe below:

I. CRISIS TRIGGER EVENT CRISIS
Crisis Detection
Physical Security Unit of Red Eléctrica de España, S.A.U.
Agents involved
The following agents involved have been identified: Red Eléctrica de España, S.A., the Distribution System Operators (DSO), Generation Companies, State Security Forces and Bodies (FCSE), Official Bodies (National Center for the Protection of Critical Infrastructures (CNPIC), National Institute of Cybersecurity of Spain (INCIBE), Cybersecurity Coordination Office (OCC), Ministries).
II. MEASURES TO BE ADOPTED DURING THE CRISIS
Preventive measures at national level
Steps that can be taken before the crisis include: • Carry out physical and electronic perimeter security • Establish and apply job protection measures • Carry out access control for people and vehicles (including authentication) to the critical assets in question. • Carry out user registers of control centers • Apply and review privilege management

- Have back up elements
- Have an active redundant Control Center

Mitigating or response measures at national level

Actions to be taken during the crisis include the following:

a) System Operation Measures:

- Application of technical restrictions in real time to manage frequency deviations outside the established limits
- Generation management through generation redispatches
- Adaptation of exchange programs with France, Portugal, Andorra and Morocco
- In the event of remote control loss, allocation of field personnel to critical Electrical Substations and dispatch of instructions and communication with agents via telephone.
- Additional measures for voltage control depending on the different demand scenarios
- Return of discharges
- Manual load shedding
- Automatic load shedding by underfrequency mechanisms and schemes: it includes the disconnection of pumping groups and later preselected load shedding
- Automatic overfrequency control mechanisms and schemes: includes automatic generation disconnection plan

b) Other measures:

- Activation of the SES-OCC-FCSE Communications Protocol (Secretary of State for Security - Cybersecurity Coordination Office - State Security Forces and Bodies)
- Activation, where appropriate, of the operator's safety plans. The Interlocutor with whom communications will be maintained within the scope of this plan is the National Center for the Protection of Critical Infrastructures (CNPIC).
- Activation of Specific Protection Plans. The Interlocutor with whom communications will be maintained within the scope of this plan is the CNPIC and there will also be communications with the State Security Forces (FCSE)
- Activation of the Operational Support Plans. The deployment actions will be carried out by the FCSE

Preventive meausres at regional level

There are no preventive measures at the regional level for this type of electricity system crisis scenarios.

Mitigating or response measures at regional level

Measures that can be taken during the crisis, when it has cross-border impact, include the following:

- Carry out active power support exchanges with neighboring TSOs
- Support procedure of the Spanish and French systems for the restoration of service after generalized incidents
- Support procedure of the Spanish and Portuguese systems for the restoration of the service after generalized incidents

III. IMPACT

The crisis is expected to have an impact on consumers, Distribution System Operators (DSO), Generators, as well as, in the case of a regional crisis, in neighboring TSOs.

IV. EX-POST EVALUATION AND IMPROVEMENT

In this regard, actions to be taken include:

- Carry out analysis and correlation of events to reconstruct the sequence of events.
- Preapre report, which includes lessons learned and improvement actions
- Participate in international work groups for the analysis of incidents (eg. European Network of Transport System Operators (ENTSOe))

4.9 Forest fire

As mentioned before, wildfire scenarios are considered situations in which the incident is unintentional. However, taking into account its seriousness, serious impacts at regional level be cannot be ruled out and are in fact possible.

In this scenario, the initiating event in this type of crisis in the electricity sector is a forest fire that may affect the operation of critical facilities / assets or, where appropriate, strategic for the operation of the system.

The impacts that are most likely to occur as a consequence of this type of crisis are fundamentally:

- That there is damage to critical or strategic assets
- The unavailability of critical or strategic facilities/assets occurs as a consequence of the fire.

When analysing cross-border impacts for this type of crises, it is considered possible that fires could occur affecting Spain and Portugal. As a consequence of the same Unavailability of interconnection lines. This cross-border impact would fundamentally manifest itself in losses of the interconnection lines, if these are the assets that have suffered the incident.

The most recent example to this type of crisis is the fire in the Eastern Pyrenees below the electrical interconnection lines on July 24, 2021 in France, which led to the decoupling of the Spanish-Portuguese electrical system from the European system.

The main characteristics of this crisis scenario and the actions that are to be taken in it are describe below:

I. CRISIS TRIGGER EVENT CRISIS
Crisis Detection
The Fire Protection services of the corresponding Autonomous Communities.
Agents involved
The following implicated agents have been identified: Red Eléctrica de España, SA, the Distribution System Operator (DSO), Generation Companies, State Security Forces (FCSE), Fire Protection Services, Emergency Military Unit (UME), Official Bodies (National Center for the Protection of Critical Infrastructures (CNPIC), Ministries).
II. MEASURES TO BE ADOPTED DURING THE CRISIS
Preventive measures at national level

Steps that can be taken before the crisis include:

- Cancel reclosures of lines/units
- Carry out personnel allocatino to identify affected lines and open lines.

Mitigating or response measures at national level

Actions to be taken during the crisis include the following:

a) System Operation Measures:

- Application of technical restrictions in real time to manage frequency deviations outside the established limits
- Generation management through generation redispatches
- Adaptation of exchange programs with France, Portugal, Andorra and Morocco
- In the event of remote control loss, allocation of field personnel to critical Electrical Substations and dispatch of instructions and communication with agents via telephone.
- Additional measures for voltage control depending on the different demand scenarios
- Return of discharges
- Manual load shedding
- Automatic load shedding by underfrequency mechanisms and schemes: it includes the disconnection of pumping groups and later preselected load shedding
- Automatic overfrequency control mechanisms and schemes: includes automatic generation disconnection plan

b) Other measures:

- Activation of the SES-OCC-FCSE Communications Protocol (Secretary of State for Security - Cybersecurity Coordination Office - State Security Forces and Bodies)
- Activation, where appropriate, of the operator's safety plans. The Interlocutor with whom communications will be maintained within the scope of this plan is the National Center for the Protection of Critical Infrastructures (CNPIC).
- Activation of Specific Protection Plans. The Interlocutor with whom communications will be maintained within the scope of this plan is the CNPIC and there will also be communications with the State Security Forces (FCSE)
- Activation of the Operational Support Plans. The deployment actions will be carried out by the FCSE

Preventive meausres at regional level

Carry out the adaptation of exchange programs with neighboring Member States, as well as with neighboring third countries

Mitigating or response measures at regional level

Measures that can be taken during the crisis, when it has cross-border impact, include the following:

- Carry out active power support exchanges with neighboring TSOs
- Support procedure of the Spanish and French systems for the restoration of service after generalized incidents
- Support procedure of the Spanish and Portuguese systems for the restoration of the service after generalized incidents

III. IMPACT

The crisis is expected to have an impact on consumers, Distribution System Operators (DSO), Generators, as well as, in the case of a regional crisis, in neighboring TSOs.

IV. EX-POST EVALUATION AND IMPROVEMENT

In this regard, actions to be taken include:

- Carry out analysis and correlation of events to reconstruct the sequence of events.
- Preapre report, which includes lessons learned and improvement actions
- Participate in international work groups for the analysis of incidents (eg. European Network of Transport System Operators (ENTSOe))