ΡΥΘΜΙΣΤΙΚΗ ΑΡΧΗ ΕΝΕΡΓΕΙΑΣ
REGULATORY AUTHORITY FOR ENERGY

Risk Preparedness Plan for the Electricity Sector of Greece

In line with the provisions of Regulation (EE) 2019/941 of the European Parliament and of the Council of 5th June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC

ATHENS

August 2022

Table of Contents

List of tables

List of Figures

Acronyms

AC:	Alternating Current
ACER:	Agency for the Cooperation of Energy Regulators
CSIRT:	Computer Security Incident Response team –Cybersecurity Directorate HNDGS
DC:	Direct Current
ECG:	Electricity Coordination Group
EENS:	Expected Energy Non Served
ENTSO-E:	European Network of Transmission System Operators
HVDC:	High Voltage Direct Current
LOLE:	Loss of Load Expectation
RCC:	Regional Coordination Center
RSC:	Regional Security Coordinator
SAFA:	Synchronous Area Framework Agreement
SEE SOR:	Southeast Europe System Operation Region
DPA:	Data Protection Authority
IPTO:	Independent Power Transmission Operator
RES:	Renewable Energy Sources
GSCP:	General Secretary for Civil Protection
DAPEEP:	Renewable Energy Sources Operator & Guarantees of Origin
HEDNO:	Hellenic Electricity Distribution Network Operator
DESFA:	National gas transmission system operator
DSO:	Distribution System Operator
TSO:	Transmission System Operator
En.Ent:	Energy Entity
NCA:	National Cybersecurity Authority
HNMS:	Hellenic National Meteorological Service
NPHO:	National Public Health Organization
CCEM:	Coordination Committee for Emergency Measures
HETS:	Hellenic Electricity Transmission System
HEnEx:	Hellenic Energy Exchange

RLY: Relay

GC: Grid Code

DNCC: Distribution Network Control Centre

UHVC: Ultra High Voltage Centre

CMU: Crisis Management Unit

NIIs: Non-Interconnected Islands

CRG: Crisis Response Group

RMG: Risk Management Group

CMG_{Elec}: Crisis Management Group for Electricty

RAWG: Risk Assessment Working Group

RAE: Regulatory Authority for Energy

S/S: Substation

ISM: Information Security Manager

RMT: Risk Management Team

N.G: Natural Gas

Introduction

Scope

The Regulation (EE) 2019/941 of the European Parliament and of 5th June 2019 Council on risk-preparedness in the electricity sector and repealing Directive 2005/89/EK (hereafter the «Regulation»), introduces a common framework for the prevention, preparedness and management of electricity crises.

According to Article 12 of Law 4001/2011 (Gov. Gazette A' 179/22.08.2011), as modified by Article 143 of Law 4819/2021 (Gov. Gazette A' 129/23.07.2021), **RAE was appointed as Competent Authority** according to the provisions of Article 3 of the Regulation.

According to the provisions of Article 7 of the Regulation, RAE, within the scope of its responsibilities, conducted a study with the goal of identifying the national electricity crisis scenarios for the Interconnected System of Greece. The above study was forwarded to the Commission and the ECG on 29.04.2022.

Based on this study, RAE drafted the current Risk Preparedness Plan for the Electricity Sector of Greece (hereafter the «Plan»), according to the provisions of articles 10, 11, 12 and Appendix of Regulation.

The scope of the Plan is to identify potential risks related to the security of electricity supply and to highlight the existing and planned measures to prevent and manage of those risks.

For the Plan's drafting, RAE cooperated with the Independent Transmission System Operator (IPTO), with contribution from the following parties:

- The Operator of the Hellenic Electricity Distribution Network (HEDNO),
- The Hellenic Energy Exchange (HEnEx),
- The General Directorare of Cybersecurity of the Hellenic Ministry of Digital Governance.

Finally, for the completion of the Plan, RAE consulted extensively with all involved parties.

According to Article 11 of the Regulation, the Plan includes the following:

- ✓ Short description of the technical characteristics of the interconnected transmission system of Greece, as well as of interconnections with neighbouring countries.
- ✓ Quick summary of risk criteria that were adopted for the identification of risks.
- ✓ Presentation of risks that were simulated and categorized based on impacts and likelihood of occuring and resulted in the identification of national risk scenarios.
- ✓ Summary description of national electricity risk scenarios.
- ✓ Detailed description of the roles and responsibilities of the Competent Authority.
- ✓ Description of roles of risk management bodies.
- ✓ Description of roles of electricity crisis management bodies.
- ✓ Designation of the crisis coordinator and description of his roles.
- ✓ Detailed description of electricity crisis management mechanisms based on identified national risk scenarios.
- ✓ Description of the information flow between involved parties and entities during a possible electricity crisis.
- ✓ Description of national, regional and bilateral procedures and measures taken, to prevent or face and mitigate the consequences of an electricity crisis.

The Plan is updated every four years and, if circumstances arise, more frequently.

Structure

The plan presented currently in this text follows in general the template that is described in the Appendix of the Regulation and its structure is as follows:

In ***Introduction*** the goal and a summary of the Plan's content are presented, information regarding the technical characteristics of the interconnected transmission network of Greece and interconnections with neighboring countries and countries within the same region are identified.

In ***Chapter 1*** the goal is to briefly present all national crisis scenarios that RAE identified, based on the result of the conducted study according to Article 7 of the Regulation. Towards this direction, firstly, the Risk Criteria are presented, that were adopted for identification and evaluation of risks related to the security of electricity supply. Secondly, the definition of an electricity crisis is determined in clarity, along with the national crisis scenarios that were determined and are correlated with the above risks as well as regional scenarios determined by ENTSO-E, under Article 6 of the Regulation. National crisis scenarios with similar characteristics are combined and classified into five groups (clusters), followed by a brief description for every scenario and reference to potential impact on national and cross-border level. Finally, the classification of national crisis scenarios, based on their impacts and possibility of occurrence, is presented and an assessment of risk is made as well as categorization based on risk factor and risk tolerance of each scenario.

In ***Chapter 2,*** firstly, the role and responsibilities of the Competent Authority (RAE) are described in detail, based on Regulation's provisions. Then, the bodies responsible for risk managing the security of electricity supply are introduced and their roles are described.

Additionally, new bodies are introduced with the following responsibilities: issuing early warnings of upcoming electricity crisis, declaring state of electricity crisis as well as the successful management of such a crisis. Also, their roles are described.

Information flow and interactions between all involved parties are thoroughly presented and reflected in respective diagrams. Special reference and description of the above is also made for the case of cyberattack incidents, where involvement of multiple entities is required for effective management of the crisis. Lastly, the Crisis Coordinator is defined, and its role is described.

In ***Chapter 3*** a description is given of all national measures, related to prevention or facing and mitigating impacts caused by an electricity crisis. At first, general measures taken by IPTO are presented along with actions to stabilize the System within safe operational bounds. Then, explicit national measures are presented for each of the five groups (clusters), in which all scenarios where classified. Also, existing regional and bilateral measures are included, which were taken by IPTO in agreement with neighboring countries' TSOs.

In ***Chapter 4*** all information is provided, regarding conducted consultation with involved parties from the internal electricity market, as well as Competent Authorities of neighboring Member States of the region.

Finally, in ***Chapter 5*** the framework of tests is presented, which are conducted every two years and focus on evaluating the effectiveness of the Plan and specifically of measures and procedures related to prevention and management of electricity crisis incidents. Tests on the ability of the system to manage cyberattacks, are of great importance for the country.

Hellenic Electricity System

α. Technical description of the electricity transmission system

The Hellenic Electricity Transmission System (HETS) consists of the Interconnected System of Mainland Greece and all interconnected with it islands to the High Voltage System. The HETS includes transmissions lines (overhead, underground and submerged) in high (66 kV, 150kV) and ultra-high voltage (400kV) as well as ultra-high voltage centers (UHVC) and substations of the system (SS) where transformers are used to step-up or down voltage. In more detail, Table 1 displays data related to transmission lines of HETS.

Table 1. *Length of Transmission lines of the System*

Voltage Level (kV)	Type TL	Total Length (km)	Total
66	Overhead	39	
	Submerged	74	113
150	Overhead	8047	
	Underground	267	
	Submerged	487	9570
400	Overhead	2760	
	Underground	31	
	Overhead DC	107	
	Submerged DC	160	3040
Total			**11954**

The system contains a total of 25 UHVC. 14 of them are connection points with the 400kV and 150V systems to transport electricity to the 150kV system. The remaining 11 UHVC, are neighboring electricity power plants in order to elevate voltage from plants to the 400kV Voltage Level. Moreover, 356 high-voltage substations are used to further step-down voltage in the system.

β. International Interconnections

The HETS operates synchronously and in parallel with the European System under the coordination of ENTSO-E. Parallel operation of HETS with the European System is achieved through interconnected transmission lines with the Systems of Bulgaria, Albania, North Macedonia and Turkey. Additionally, the HETS is connected asynchronously with Italy using a submerged direct current connection at 400kV voltage level. In more detail, the international interconnections of Greece with neighboring countries are:

- Two separate 400kV lines , single circuit and total nominal transmission capacity of 2800MVA with North Macedonia.
- One 400kV line, single circuit of 1400MVA nominal transmission capacity and one line 150kV of 138MVA nominal capacity with Albania.
- One 400kV line of 1400MVA nominal transmission capacity with Bulgaria.
- One 400kV line of 2000MVA nominal transmission capacity, double circuit with Turkey.
- One DC submerged cable 400kV of 500MW nominal capacity with Italy.

A second 400kV line with Bulgaria is under construction. The following figure displays the topology of existing and under development interconnections with the Transmission System of Balkan Countries.

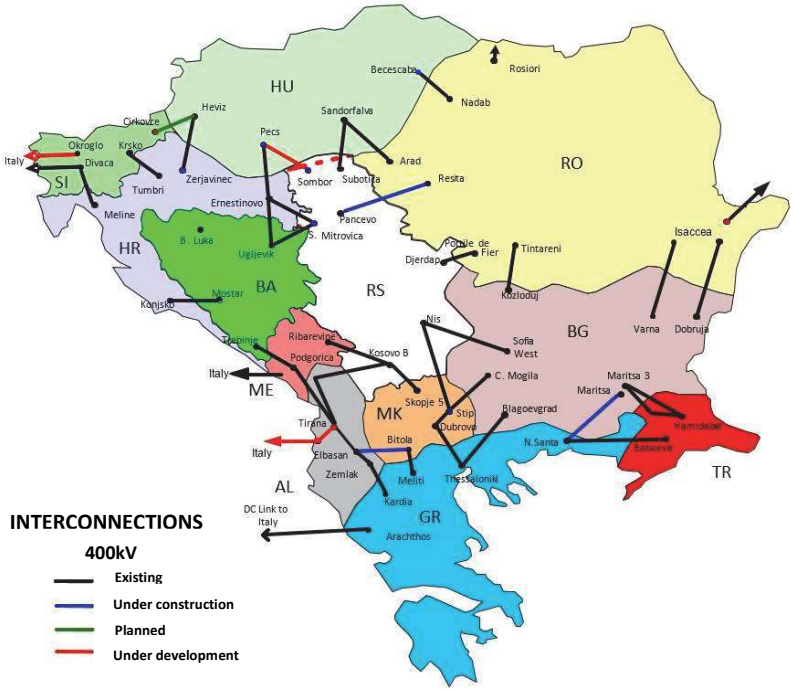

Figure 1. *Schematic diagram of the Interconnected Systems of Balkan Region.*

Member States in the region

Greece is part of the Southeast Europe System Operation Region – SEE SOR), according to ACER's decision No. 05/2022.

This region includes the following Member States:

- Italy
- Bulgaria

1. Summary of the electricity crisis scenarios

1.1 Introduction

In April 2022, the Study on identification of the national electricity crisis scenarios for the Interconnected System of Greece was completed, in accordance with provisions of Article 7 of the Regulation. The aim of the Study was to identify the conditions under which the security of electricity supply of the country would be endangered during the years 2021-2024. The results will be used as the basis for the preparation of the National Risk preparedness Plan for the Electricity Sector, according to Article 10 of the Regulation.

Considering the peculiarities of the Electricity Systems of the Non-Interconnected Islands (NIIs) and the importance of ensuring security of supply for those islands, as is for the Interconnected System, RAE is willing to conduct a distinct study to determine the crisis scenarios for the electricity supply of NIIs.

The study was conducted by RAE, in the framework of its responsibilities as Competent Authority, according to provision of par. 4 of Article 12 of Law 4001/2011 (Gov. Gazette A' 179/22.08.2011), in close cooperation with the Independent Power Transmission Operator (IPTO) and the assistance of the Hellenic Electricity Distribution System Operator (HEDNO), the Hellenic Energy Exchange (HEnEx) and the General Directorate of Cybersecurity of the Ministry of Digital Governance.

The Study was based on the methodology of ENTSO-E «Methodology for Identifying Regional Electricity Crisis Scenarios in accordance with Article 5 of the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on risk preparedness in the electricity sector and repealing Directive 2005/89/EC», which was developed according to provisions of article 6 of Regulation and approved by ACER's decision no. 07/2020.

1.2 Risk Criteria

The Study on determining the national electricity crisis scenarios, with the aim of evaluating the identified risks and supporting decision making in the process, has adopted three (3) basic criteria which the Authority values as necessary for the System to operate securely. The following were considered to define the criteria:

- The conditions that could affect the security of electricity supply.
- The method used to define and quantify impacts and the likelihood of occurence of crisis scenarios.
- The duration of crisis scenarios.
- The method of determining the impact level of scenarios (impact scale).
- The provided capabilities of allocating resources for the security of supply.

Based on the above, the adopted risk criteria are the following:

- *Security Criterion N-1[1], according to article 3 of Regulation (EE) 2017/1485:* Non violation of N-1 condition in any case.

[1] Regulation (EE) 2017/1485, article 3 paragraph 14 *«**criterion (N-1):** the rule according to which the elements remaining in operation within a TSO's control area after occurrence of a contingency are capable of accommodating the new operational situation without violating operational security limits»*

- *The adequacy of the system in conjuction with likelihood of occurence* (based on the european resource adequacy assessment conducted by ENTSO-E, in accordance with article 23 of Regulation (EE) 2019/943):
  - Expected Energy Non-Served, EENS < 0,01 %. This index refers to annual energy or annual percentage of energy the electricity production system cannot satisfy.
  - Loss of Load Expectation, LOLE < 12 h. This index refers to annual hours for which the electricity production system cannot fully satisfy demand, regardless of the deficit size for each hour.
- *Cybersecurity*: Impact rating < Critical or disastrous. The methodology for classifying impact is under development by ACER. Until a common impact rating scale is adopted for the energy sector, RAE will adopt time of detection of the cyberattack, recovery – management of attack and leak of classified data as basic criterias.

1.3 Definition of Electricity crisis

The evaluation of the importance of risks is related to their capability of causing an electricity crisis, namely significant shortages or inability to supply electricity to customers. In close correlation with the aforementioned risk criteria, the electricity crisis is defined along with the conditions, whose violation would trigger emergency measures. Thus, when identifying National Crisis Scenarios, the following definition was adopted:

- ✓ **State of crucial shortage of electrical energy or inabillity to supply customers that could lead to declaration of Early Warning or has led to Emergency in case of:**
  α) violation of N-1 standard or/and
  β) EENS ≥ 0,01 (% of annual demand) and LOLE ≥ 12 (hours) or/and
  γ) cyberattack incident with the following consequences:
  - **Disruption in supply, load outages – impact on cross-border trade.**
  - **Economic impacts, resulting in operational disruption of businesses, market manipulation.**
  - **Leakage of personal data, that can result in a significant fine by the Data Protection Authority.**

1.4 Risk identification

In order to identify conditions which could form and affect the security of supply of the Interconnected System of Greece with electricity between 2021 and 2024, RAE drafted, based on Chapter II of the Regulation in close cooperation with IPTO, an apt questionnaire of risk factors that was answered by involved parties, such as the Hellenic Distribution Network Operator (HEDNO), the Natural Gas System Operator (DESFA), Natural Gas Distribution System Operators, Power producers, Natural gas Suppliers and DAPEEP S.A., according to their experience in developing a list of risks to their area of responsibility / area of operations. In this context, involved parties contributed to the development of a list of risks by determining:

- estimated conditions, which according to their opinion, can facilitate materialization of those risks,
- the description of the initial state of the system for each crisis scenario,
- the period or yearly periods during which they believe that a crisis scenario will happen and the type of affected load,
- the estimated duration of the crisis scenario, and

- the description of potential consequences of a crisis scenario

On the basis of the methodology above, all available elements and information, that where collected through the questionnaire to determine and analyze risks which could affect the security of supply of Greece, were analyzed, as shown in Figure 2.

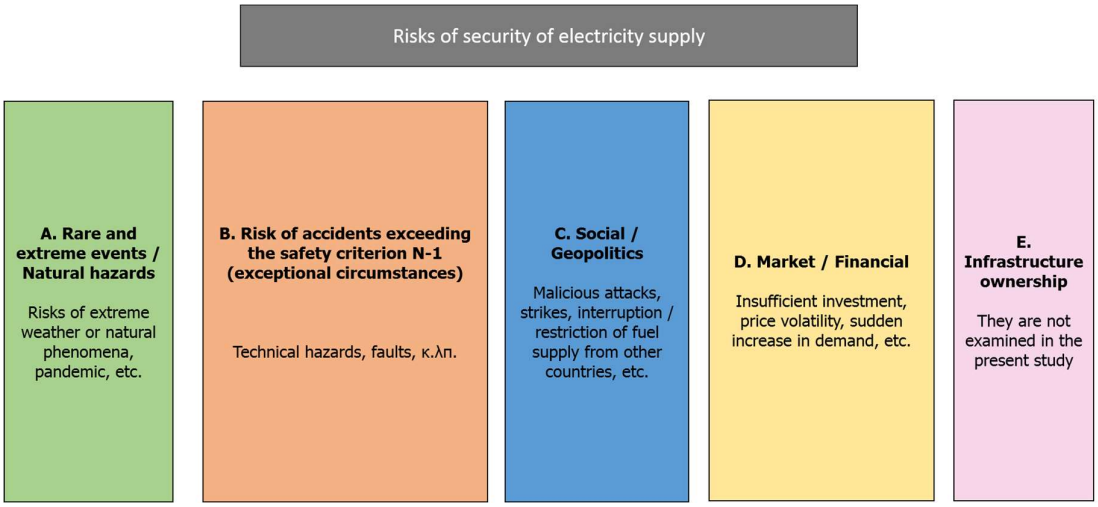

Figure 2. *Risks of security of electricity supply (Source: Study on identification of the national electricity crisis scenarios, RAE 2022)*

It should be mentioned that the Study on identification of national crisis scenarios did not evaluate risks related to the ownership of the infrastructure regarding security of electricity supply.

1.5 Determination of National Crisis Scenarios

Based on the results of the consultation for risk identification, the analysis of national and regional conditions, the results of the study of ENTSO-E on identification of Regional Electricity Crisis Scenarios (Table 2), and in accordance with article 5 of the Regulation, **16 crisis scenarios** were determined, examined and simulated in cooperation with IPTO. Depending on each scenario, the crisis was considered to last from a few hours to one (1) month, along with specific demand profiles (I – high), (II – average) and (III – low).

Table 2. *Overview of Regional Electricity Crisis Scenarios according to ENTSO-E*

A/A	Type of Regional Scenario
1	Cyberattack – Elements connected to the electricity grid.
2	Cyberattack – Elements not connected to the electricity grid.
3	Sabotage – critical infrastructure
4	Sabotage – control centers
5	Threat to key employees
6	Insider attack
7	Solar storm
8	Volcanic Eruption
9	Storm
10	Cold wave
11	Rain and floodings

12	Winter weather conditions
13	Fossil fuel shortage (incl. Natural Gas)
14	Shortage of nuclear fuel
15	Local technical failure
16	Multiple failures cause by extreme weather conditions
17	Loss of IT/COM systems for real-time operation
18	Multiple concurrent failures
19	Complexity of Power control mechanism of the system
20	Human error
21	Undesirable power flows
22	Equipment damage
23	Strikes, unrest, industrial actions
24	Industrial / Nuclear accident
25	Unpredictable interaction of energy market rules
26	Unusual and high errors in estimation of RES production
27	Pandemic
28	Heat Wave
29	Period of Drought
30	Earthquake
31	Forest fire

The results of risk identification, that were presented in the previous chapter, were the basis for determining the national risk scenarios for the security of electricity supply of Greece, as well as estimating the likelihood of occurrence. The main correlations of the crisis scenarios of electricity supply with the risks presented above, are determined in Table 3.

In Table 4, all examined scenarios are briefly presented along with their basic characteristics. To perform accurate simulation of scenarios, real-time data from specific hours and dates were selected (load, energy mix, availability of units, system topology, RES production, interconnections' schedules, etc.) Additionally, the scenarios were selected based on the particularities of the Hellenic transmission system (Peloponnese without 400kV grid, interconnections located North – demand located South).

Assumptions for each scenario, its evolution, the detailed description and analysis of every scenario are all included in the Identification of Nation Electricity Crisis Scenarios.

Finally, in Table 5, the 16 National Crisis Scenarios are matched with the Regional Crisis Scenarios identified by ENTSO-E.

Table 3. Basic risk correlation with crisis scenarios.

	Risks / Scenarios →	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16
A	Heavy rains - Flood	X															
	Extreme Winds/Storm		X	X													
	Frost – Cold wave - Snow				X						X		X	X			(X)
	Period of drought					X											
	Forest fires					X											
	Heatwave					X	X					(X)					
	Earthquake							X	X								
	Consequential risks of fuel shortage – restrictions in electricity production				(X)	(X)	(X)				(X)		X	X			X
	Pandemic									X	X						
B	Technical problems in electricity interconnections with other countries			(X)	(X)				(X)	(X)							
	Technical failure of national electricity transmission system or/and distribution system	(X)	(X)	(X)	(X)	(X)		(X)	(X)	(X)		X					
	Technical failure of important grid element	(X)	(X)	(X)	(X)	(X)		(X)	(X)	X		X					
	Simultaneous loss of important grid elements	(X)	(X)	(X)	(X)	(X)		(X)	(X)	(X)		X					
	Technical failure of upstream interconnected natural gas transmission systems or/and domestic transmission system				(X)												(X)
	Malfunction of IT/COM Systems (Information Technology και Communications)														(X)	(X)	
	Human Error									X					(X)	(X)	
	Terrorist attacks														(X)	(X)	
	Vandalism/Sabotage to the electricity transmission and/or distribution system																
	Strikes in related sectors with long duration																
	Threat / Blackmailing / Hostage-taking of employees																
	Internal attack																
	Cyberattacks														X	X	
	Geopolitical risks														(X)	(X)	X
Δ	Conventional – commercial dispute																
	Underinvestment/lack of infrastructure/delayed development of important infrastructure									(X)	(X)		X				(X)
	Price volatility				(X)								X	X			(X)
	Sudden and unexpected rise of peak demand		(X)		(X)	(X)	(X)				(X)	(X)	X	X			
	Possible Manipulation of energy prices in the electricity market				(X)										(X)	(X)	(X)

X: main reference, (X): secondary reference

***Table 4**. Basic characteristics of electricity crisis scenarios*

Scenario	Title of Scenario	Scenario duration	Time period	Load
S1	Floods	2 weeks	Winter	II
S2	Windstorms (Winter)	1 week	Winter	I
S3	Windstorms (Summer)	1 week	Summer	I
S4	Cold wave - Snow	2 weeks	Winter	I
S5	Droughts – Forest fires	3 weeks	Summer	I
S6	Heatwave – Maintenance of upstream natural gas network	10 days	Summer	I
S7	Earthquake	3 weeks	Summer	II
S8	Earthquake - /wo HVDC interconnection with Italy	3 weeks	Summer	I
S9	Pandemic – Human Error	As long as lockdown measures are in place, scenario dur. 1 day	Summer ι	III
S10	Decommissioning of lignite plants – Delay in commissioning of new plants	2 weeks	Winter (2022-2023)	I
S11	Equipment damage	6 hours	Summer	I
S12	Decommissioning of lignite plants – Crete Interconnection – Ptolemaida V plant not commissioned yet	1 month	Winter (2024-2025)	I
S13	Decommissioning of lignite plants – Crete Interconnection – Ptolemaida V plant commissioned	1 month	Winter (2024-2025)	I
S14	Cyberattack A	2 hours	Summer	I
S15	Cyberattack B	5 hours	Winter	I
S16	Stop of Russian gas flow	3 months	Winter (1/1/2023-31/3/2023)	I

***Table 5.** Matching of national crisis scenarios with regional scenarios identified by ENTSO-E*

National Crisis Scenarios	Regional Crisis Scenarios
S1. Floods	**No. 11** Heavy precipitation and flooding
S2. Windstorms (Winter)	**No. 9** Storm
S3. Windstorms (Summer)	
S4. Cold wave – Snow	**No. 10** Cold Wave
S5. Drought – Forest fires	**No. 29** Period of drought & **No. 31** Forest fire
S6. Heatwave – Maintenance of upstream natural gas network	**No. 28** Heatwave & **No. 15** Local technical failure
S7. Earthquake	**No. 30** Earthquake

S8. Earthquake – /wo HVDC with Italy	**No. 30** Earthquake & **No. 22** Equipment damage
Σ9. Pandemic – Human Error	**No. 27** Pandemic & **No. 20** Human Error
Σ10. Decommissioning of lignite plants – delay in the commissioning of new plants	
Σ11. Equipment failure	**No. 18** Multiple simultaneous failures
Σ12. Decommissioning of lignite plants – Crete Interconnection – Ptolemaida V plant not commissioned yet	
Σ13. Decommissioning of lignite plants – Crete Interconnection – Ptolemaida V plant commissioned	
Σ14. Cyberattack A	**No. 2** Cyberattack – Elements not connected to the grid
Σ15. Cyberattack B	**No. 1** Cyberattack – Elements connected to the grid
Σ16. Stop of Russian gas flow	**No. 13** Shortage of fossil fuels (incl. Natural Gas)

1.6 Summary of National Electricity Crisis Scenarios

Below follows a brief description for each of the 16 national electricity crisis scenarios, the initial incident responsible for the crisis situation, the evolution and the potential consequence of each scenario at national level as well as regional level (if any). Crisis scenarios with similar characteristics were joined and categorized in groups (clusters) for a more efficient management of related measures of prevention and treatment and will be presented in chapter 3. Therefore, national crisis scenarios are categorized as follows:

- Malicious attacks
- Natural Hazards
- Pandemic / Human Error
- Shortage of fossil fuels
- Failures of the electrical grid

1.6.1 Cyberattacks

S14. Cyberattack A

In this scenario, cyberattacks on crucial subsystems of the Hellenic Energy Exchange (HenEx) are examined, with the following consequences: shutdown of operations or suspension of the stock market, possibility of corruption of transaction data, significant financial losses for participants, reputational damage of HenEx, etc.

S15. Cyberattack B

In this scenario, cyberattacks on crucial infrastructure and system of an energy entity, connected to the grid, are examined. In general, these are referred to systems of IPTO (energy management system, automated production adjustment system, market solver system, load

– frequency control system, market management system, real-time market balancing, etc), systems of HEDNO (distribution management system, metering systems, grid telemetry and supervision systems, etc), systems of power producers or/and other energy entities. Such incidents could threaten the security of supply of the country, with the extreme case of a blackout.

1.6.2 Natural Hazards

S1. Floods

Extreme rainfall after a long period of drought, can result in river overflows, collapse of embankments and ground erosion. As a result, possible incidents of S/S flooding and serious damage to foundations of pylons of transmission lines, underground networks and equipment of S/S & HVC can occur. Parallel operation of hydroelectric facilities aggravates the situation, while possible interruption of their operation poses risks to the smooth supply of the surrounding region. Additionally, it is likely that the capability of production units to offer balancing services will be reduced, as well as the ability of the competent operator to redispatch units and it is considered probable that preventive equipment isolations will be performed for safety reasons. Finally, additional support through imports of electricity might be requested by neighboring TSOs due to reduced production capacity and availability of the transmission system.

S2. & S3. Windstorms

Stormy winds with violent gusts and intensive thunderstorms that cause turbulence, tree falls etc. These conditions can appear either during winter or summer. As a result, significant damage can be caused to radial distribution grids, trigger automated protection systems of equipment, pylons of transmission lines could collapse, transmission lines cut by fallen trees or other objects, as well as a reduction of production of wind turbines due to high wind speed or their disconnection from the grid. The impact of all the above, are load outages or voltage drops locally/regionally, as well as reduction in production capacity due to the inability of the system to transport to customers. It is also considered possible that interconnections with some neighboring countries will be cut off, with subsequent increase of charging of other interconnections, without an overall reduction of scheduled energy flows. Thus, in this scenario, there are no impacts to cross-border trade.

S4. Cold wave - snow

Occurrence of extremely low temperatures, intense snow and ice in combination with high energy demand due to weather conditions. Impacts include significant damage to transmission and distribution networks, fall of circuits and damage to pylons due to accumulation of ice, reduced production of RES and hydroelectric units due to ice, reduced production of thermal units due to issues with their cooling systems, but also due to problems of transportation of LNG for their supply. Possible consequences of the above are overload of the grid, N-1 security issues and reduced transportation capability of transmission system. At cross-border level, imports of electricity are increased. Nevertheless, unavailability of interconnections and damages may appear, with the result of inability to implement cross-border transaction programs. Additionally, similar weather conditions in neighboring countries can highly increase prices of fuels/energy and limit import capability.

S5. Drought – Forest fires

Prolonged and extremely dry period during the summer, in combination with high temperatures and intense winds that facilitate starting and spreading forest fires. The fires spread uncontrollably for several days. As a result, outages of transmission and distribution lines, damage to substation equipment, power outages to affected areas and reduced availability of thermal and hydroelectric units will occur. Impacts of the above include possibility of adequacy problem and the occurrence of rotational load shedding due to inability to meet demand. At cross-border level, the need to increase support of electricity supply from neighboring TSOs is expected. In a worst case, the risk of becoming an "energy island" from the rest of synchronous area is looming.

S7. & S8. Earthquake

Due to a powerful earthquake, pylons of transmission lines, poles of the distribution network and substation equipment are damaged. Additionally, damages to power plants' equipment affect their availability, resulting in downgrading of the structure and control of the transmission system. Unusual load flows are expected to appear due to the unavailability of crucial system elements, while the repair process is likely to be delayed due to damages to other infrastructure (e.g. road network). At cross-border level, in case of significant damage to interconnections, the ability to exchange energy will be limited. Specifically for Scenario No. 8, (S8), the ability of other countries to support through increased imports is severely limited.

1.6.3 Pandemic / Human Error

S9. Pandemic – Human Error

In this scenario, a new pandemic affects the whole world, resulting in supply chain disruptions, absences of specialized personnel due to sickness with the remaining personnel operating under stressful conditions and the appearance of «human error», in the form of an untimely assessment of the risks for the system and poor handling of the repair process of damages. As a result, major deviations between forecasted and real load appear and imbalances that cannot be met by reserves. At cross-border level, trade is affected due to inability to forecasted load, which in a worst case can lead to significant failures and major imbalances and as a result «islanding» of the system.

1.6.4 Shortage of fossil fuels

S6. Heat wave – Maintenance of upstream natural gas network

This scenario includes prolonged period of heat (longer than ten days) combined with scheduled maintenance of the upstream natural gas network, and as a result reduced natural gas imports. Additionally, due to weather conditions the demand is high, production from RES is reduced due to low wind speeds, the level of water reservoirs of hydroelectric units is low, while efficiency of thermal units and natural gas power plants is reduced. Considering the above, reserves are activated and fully used in a short time frame, congestion appears at interconnections and in general voltage imbalance and power adequacy issues emerge. At

cross-border level, the need to increase support of electricity supply from neighboring TSOs is expected, while limitations in energy exchanges due to reduced transporting capability of the internal transmission system are possible.

S10. Decommissioning of lignite plants – delay of commissioning of new plants

In this scenario, all lignite plants are decommissioned in the context of the implementation of the policy to reduce the environmental footprint of electricity, while at the same time other factors delay the commissioning of new units in the system. This leads to power adequacy issues, the inability to secure necessary reserves, overloading of transmission lines due to new grid topology resulting in increased chances of failures and activation of emergency measures (e.g. rotational load shedding). At cross-border level, possible limitations on traded quantities can be expected and the need for support by neighboring states arises in terms of active power and ancillary services.

S12. & S13. Decommissioning of lignite plants – Crete Interconnection – With / Without Commissioning of Ptolemaida V plant

In this scenario, a combination of factors at national level is examined that includes simulation of the system, provided that all lignite plants are decommissioned, the interconnection of Crete with mainland Greece is completed, the commission of the new power plant Ptolemaida V is completed or not. As a result, power adequacy issues are expected, possible inability to secure necessary reserves for the system, as well as inability to export electricity during daily peak demand, imposed limitations on cross-border trade and a need for increased support by neighboring countries.

S16. Stop of Russian gas flow

In this scenario, a complete stop of natural gas flow from Russia is examined, in the context of the recent geopolitical events and the Russian invasion of Ukraine. The scenario includes a series of combined assumptions, resulting in impacts at national level (adequacy issues, rotational load shedding) and at cross-border level, as there is a high probability of impact on balance sheet, considering the crisis conditions all over Europe.

1.6.5 Failures in the electricity system

S11. Equipment failure

This scenario includes a combination of incidents, specifically the simultaneous occurrence of two failure and different causes, affecting the security of operation of the system in a specific geographical area. Those failures can lead to consequences such as unchecked tripping of breakers, overload of transmission lines, exceeding of thermal limits, loss of production unit, deficiency of active and reactive power, instability of the system, as well as potential collapse of the system locally or totally. No significant impact at cross-border level.

1.7 Classification of Impacts of Crisis Scenarios

Impacts of examined scenarios (S1-S13 and S16) on the transmission system were rated according to the 5 scale levels of Appendix I approved by ACER (decision No 07/2020) methodology of ENTSO-E, using two parameters, the "Expected Energy Not Served" – EENS and the "Loss of Load Expectation" – LOLE, as shown in the following table.

Table 6. *Classification of impact of crisis scenarios*

Impact classification	EENS (%) (of annual demand)	LOLE (hours)
Disastrous	≥ 0,25	≥ 168
Critical	≥ 0,05 και < 0,25	≥ 48 και < 168
Major	≥ 0,01 και < 0,05	≥ 12 και < 48
Minor	≥ 0,002 και < 0,01	≥ 3 και < 12
Insignificant	< 0,002	< 3

Specifically, for the classification of impacts of scenarios S14 and S15, related to cybersecurity, Table 7 was created. In detail, as aforementioned, the methodology for the classification of impacts on cybersecurity is subject to the Network Code for cybersecurity and during the drafting of the Study was in the final stage of development by ACER. Thus, until the establishment of a common impact rating for the energy sector, RAE distinguishes as basic criteria the time till detection and restoration – management of the cyberattack, as well as the data leakage of confidential information. Through cooperation with examined entities, it is concluded that the crucial duration of facing a cyberattack varies significantly for each party. Therefore, a 5-scale level shown in Table 7 was used for a more qualitative rating of impacts.

Table 7. *Impact rating of cyberattacks*

Impact classification	Level of penetration affected entities - infrastructure	Leakage of Data
Disastrous	Significant cross-border impact Can lead to loss of human life	Loss of sensitive national information, which could be used maliciously by the attacker to destroy critical national infrastructure
Critical / considerable	National blackout – impact on related sectors	Partial loss of national information, which does not give significant advantage to the attacker Massive data leakage that can result in significant fines by the DPA and a massive number of lawsuits of affected subjects

Major	Issues with security of supply, load shedding – impact on cross-border energy transactions	Economic impact followed by impacts on operation of businesses, market manipulation Leakage of personal data that can result in significant fine by the DPA
Average	The problem affects other entities, measures needed outside the market	Leakage of commercial information that results in economic impact between companies in competition
Minor / insignificant	Entities deal with the problem internally	Leakage of confidential data – sensitive commercial data with negligible economic impact

Regarding classification based on likelihood of occurrence of a crisis scenario, the corresponding scale of Appendix I of aforementioned methodology of ENTSO-E was considered, which was approved by decision no. 07/2024 of ACER, and presented below in Table 8.

Table 8. *Classification of crisis scenarios based on likelihood of occurrence (ACER decision)*

Classification	Likelihood of occurrence per year	Years per occurrence	Description / example of initiating event
Very likely	≥ 50%	2 or less	Event expected practically every year, e.g. extreme wind/storms causing multiple failure of overhead lines may be expected nearly every year in some areas
Likely	20-50%	2-5	Event expected once in a couple of years, e.g. extreme heat wave causing limits on output of open-loop water-cooled power plants, low water levels at hydro plants, higher load, etc.
Possible	10 – 20 %	5-10	Event expected or taken into consideration as a potential threat, e.g. cyber or malicious
Unlikely	1-10%	10-100	Very rare event with potentially huge impact, e.g. simultaneous floods causing unavailability of generation, distribution and transmission infrastructure
Very unlikely	≤ 1%	100 or more	Event not observed but potentially disastrous, e.g. earthquake causing a huge destruction of transmission, distribution and generation infrastructure.

1.8 Risk Assessment of Crisis Scenarios

The risk assessment of each scenario was conducted by considering its impact scale combined with the likelihood of occurrence rating, presented above, which was used to create the Risk Matrix shown in Figure 3.

Impact		Likelihood				
EENS%	LOLE	Very likely	Likely	Possible	Unlikely	Very unlikely
Disastrous	Disastrous	Disastrous	Disastrous	Critical	Major	Minor
Disastrous	Critical	Disastrous	Critical	Critical	Major	Minor
Critical	Disastrous	Disastrous	Critical	Critical	Major	Minor
Disastrous	Major	Disastrous	Critical	Major	Major	Minor
Major	Disastrous	Disastrous	Critical	Major	Major	Minor
Disastrous	Minor	Disastrous	Critical	Major	Major	Minor
Minor	Disastrous	Disastrous	Critical	Major	Major	Minor
Disastrous	Insignificant	Disastrous	Critical	Major	Major	Minor
Insignificant	Disastrous	Disastrous	Critical	Major	Major	Minor
Critical	Critical	Disastrous	Critical	Major	Minor	Minor
Critical	Major	Critical	Critical	Major	Minor	Minor
Major	Critical	Critical	Critical	Major	Minor	Minor
Critical	Minor	Critical	Major	Major	Minor	Minor
Minor	Critical	Critical	Major	Major	Minor	Minor
Critical	Insignificant	Critical	Major	Major	Minor	Minor
Insignificant	Critical	Critical	Major	Major	Minor	Minor
Major	Major	Critical	Major	Major	Minor	Insignificant
Major	Minor	Major	Major	Minor	Minor	Insignificant
Minor	Major	Major	Major	Minor	Minor	Insignificant
Major	Insignificant	Major	Major	Minor	Minor	Insignificant
Insignificant	Major	Major	Major	Minor	Minor	Insignificant
Minor	Minor	Major	Minor	Minor	Insignificant	Insignificant
Minor	Insignificant	Major	Minor	Minor	Insignificant	Insignificant
Insignificant	Minor	Major	Minor	Minor	Insignificant	Insignificant
Insignificant	Insignificant	Minor	Minor	Insignificant	Insignificant	Insignificant

Figure 3. *Risk Assessment of Crisis Scenarios*

In order support decision-making, Table 9 was created to illustrate the Risk Matrix in relation to risk rating of each scenario. This definition relates risk tolerance, based on specific risk criteria as well as decision making.

Table 9. *Definition of risk levels*

Risk rating	Risk tolerance	Support in decision making
Extreme	Non tolerable	The level of risk is so significant that risk management must be imposed. At this stage, actions must be taken to mitigate risk at a lower level
Very high		
High	Non desirable	These risks require cost-benefit analysis to determine the best approach. At this stage, preventive actions must be designed to mitigate recognized risks
Average		

Low	Tolerable	Risk of this level can be defined as negligent and thus no action is required. However, active monitoring is required to maintain the risk at this level

According to the analysis of under examination crisis scenarios and the Risk Matrix created to evaluate their risk, Scenarios included in the risk group «Social – Geopolitical Risks» (namely **Stop of NG flow from Russia** and **Cyberattacks**) and «Rare and Extreme Natural Hazards» (namely **Heat wave** and **Cold wave, accompanied by intense snowfall**) are expected to have the most unfavorable impact on security of supply of consumers and make it necessary to quickly adapt existing plans and at the same time take action to prevent, treat and reduce impact from competent bodies. Thus, the following prioritization was made regarding the plan of response measures:

I. Scenarios of non-tolerable risk

1) **Scenario 16 (α)**: Stop of NG flow from Russia (winter 2022-2023 -without Ptolemaida V)
2) **Scenario 16 (β)**: Stop of NG flow from Russia (winter 2022-2023 -with Ptolemaida V)
3) **Scenario 4**: Cold wave - snow
4) **Scenario 6**: Heat wave – maintenance of upstream NG network
5) **Scenario 15**: Cyberattack B

II. Scenarios of non-desirable risk

6) **Scenario 1**: Floods
7) **Scenario 14**: Cyberattack A
8) **Scenario 9**: Pandemic – human error
9) **Scenario 5**: Drought – Forest fires
10) **Scenario 12**: Decommissioning of lignite plants – interconnection of Crete, without Ptolemaida V
11) **Scenario 11**: Equipment damage
12) **Scenario 2 και 3**: Windstorms
13) **Scenario 10**: Decommissioning of lignite plants – delay in commissioning of new plants

III. Scenarios of tolerable risk

14) **Scenario 13**: Decommissioning of lignite plants – interconnection of Crete, with Ptolemaida V
15) **Scenario 7**: Earthquake
16) **Scenario 8**: Earthquake - without HVDC cable with Italy

2. Roles and responsibilities

2.1 Competent Authority

According to article 12 of Law 4001/2011 (Gov. Gazette A' 179/22.08.2011), as amended by article 143 of Law 4810/2021 (Gov. Gazette A' 129/23.07.2021), RAE (Regulatory Authority for Energy) was appointed as the Competent Authority according to the provisions of article 3 of the Regulation. The appointment of RAE as Competent Authority, was notified to the Commission and the ECG on 10th August 2021.

RAE is an independent regulatory authority, which was established by Law 2773/1999, in the framework of harmonization with Directive 2003/54/EC and 2003/55/EC for electricity and natural gas, whose main responsibility is to monitor all sectors of the internal energy market and by adopting measures with the goal of liberalizing the electricity and natural gas markets.

To improve the efficiency of risk management of security of supply of the country with natural gas or electricity, RAE promotes the adoption of cooperation framework between involved parties which will ensure:

- The adoption of a common perception between parties of the importance of risk management.
- The participation of invloved parties in decision making, in regards to risk management, which is transparent and poses no exclusions.
- Their co-responsibility in investigating and estimating potential conditions that affect the security of supply.
- The consulation and assignment of responsibilites to involved parties in order to manage risk.
- The continuous improvement of methodologies used, tools and techniques.
- The timely provision of information from involved parties, regarding conditions that could affect the security of supply.
- The promotion of actions for the development of risk management systems.
- The cooperation with competent authorities of the countries and the European Commission.

Specifically, as competent authority, RAE is responsible with duties based on Regulation (EE) 2019/941 which include the following:

- Cooperation with competent authorities of other member states, according to Article 3(1) of Regulation 2019/941.
- Ensures that all risk related to security of supply are evaluated according to Regulation (EE) 2019/941 and Chapter IV of Reguilation (EE) 2019/943. To this purpose, according to article 4 of Regulation 2019/941, it cooperates with the transmission system operator (TSO), the distribution system operator, ENTSO-E, the regional coordination centre [2] and other relevant stakeholders.

[2] Regional Coordination Centre (RCC) will be operational by 1st of July 2022, replacing regional security coordinators (RSC), pursuant to Art. 35(2) of Regulation (EU) 2019/943 of the European Parliament and of the Council on the internal market of electricity.

- Identifies the relevant electricity crisis scenarios, following the consulation with TSO, DSO, relevant power producers or trade bodies , as stated in article 7 of Regulation (EE) 2019/941.
- Prepares the risk preparedness plan for the electricity sector in Greece, in accordance with Article 10(1) of Regulation (EU) 2019/941.
- In cases, where specific, serious and reliable information indicates that an electricity crisis will occur, RAE notifies without any delay an early warning to the Commission, the competent authorities of member states within the same region and, if not within the same region, the competent authorities of members states directly linked with, according to article 14(1) of Regulation (EE) 2019/941. This warning may include information related to the causes of a potential electricity crisis, planned or taken measures for prevention of the crisis or the need for support from other member states, as well as potential impact of the measures on the internal electicity market.
- When facing an electricity crisis, after consulting with the TSO, RAE declares a state of electricity crisis and informs without delay the Commission, the competent authorities of other member states within the same region and, if not within the same region, the competent authorities of directly linked member states according to article 14(2) of Regulation (EE 2019/941). Provived information includes the causes regarding worsening of security of supply, the reasons for declaring a state of emergency, planned and already taken measures to mitigate impact and the need for potential support from other member states..
- Informs all relevant stakeholders regarding the issuance of an early warning or the declaration of a power crisis situation.
- Informs all relevant stakeholders in Greece about the potential application of non-market based measures to manage the electricity crisis, based on article 16 of the Regulation (EE) 2019/941.
- Drafts a report ex post, which evaluates the electricity crisis, and notifies it to the Commission and ECG, which must include the minimum information stated in article 17(2) of Regulation (EE) 2019/941.
- Presents the result of the report to the ECG according to article 17(4) of Regulation (EE) 2019/941.
- Performs a revision of the existing risk preparedness plan for electricity every four (4) years, taking into account the conclusions of the above results.

2.2 Risk management bodies

To successfully manage risks, the following bodies are formed:

1. **Risk Management Group (RMG).**
2. **Risk Management Team (RMT).**
3. **Risk Assessment Working Group (RAWG).**

Structure, role and mission of the bodies mentioned above, are presented below in detail.

Risk Management Group (RMG)

The Risk Management Group is appointed as competent body and is the permanent mechanism for cooperation, consultation and communication between involved parties in risk management. Represented in the RMG are the following: RAE (Coordinator – Head of RMG), the Ministry of Environment and Energy, the Independent Power Transmission Operator (IPTO), the Operator of National Natural Gas System (DESFA). The RMG can also attend, depending on the case, representatives of other involved parties, such as HEDNO, power producers, Operators of the Distribution Systems of Natural Gas, etc., after RAE's decision. Particularly, in the context of risk management in cybersecurity, and after RAE's invitation, representatives of the Data Protection Authority (DPA), the National Cybersecurity Authority (NCA), the GR-CSIRT can participate in RMG.

It's mission is to:

- Coordinate actions for the implementation of the policy of risk management.
- Consultate on distribution of responsibilities for risk management.
- Regularly review the conditions that could affect the security of electricity supply of the country.
- Conduct a study on identification of national electricity scenarios through cooperation.
- Propose measures to mitigate risk regarding security of electricity supply of the country.
- Cooperate and prepare and Risk Preparedness Plan for the electricity sector.

The RMG will hold a meeting after RAE's invitation request (or proposal by a member of the team), on a regular basis and a minimum of two (2) times per years (right after ENTSO-E has published its seasonal studies of Winter & Summer Outlook).

Risk Management Team (RMT)

The Risk Management Team (RMT) is an executive member of RAE, who is appointed as head coordinator of evaluating procedures and risk monitoring regarding the security of energy supply, with the following responsibilities:

- List and record of risks,
- Coordinate and communicate with involved parties in order to update the list of risks,
- Coordinate the Working Group to implement actions related to the identification and analysis of risks,
- Evaluate the risks,
- Coordinate actions within RAE and relevant external etities in order to monitor risks,
- Brief the President and the Board of RAE on risks or conditions, that have been identified and have the potential to affect security of supply, examined crisis scenarios and results of their simulations, forecasted demand of Operators and the results of risk evaluation.
- File a report of operation of the risk assessment system, in the context of review by the Administration,
- Responsibility for the appropriate documentation and traceability of the information

Risk Assessment Working Group (RAWG)

The Working Group for the risk evaluation is formed by RAE's decision, when the list of risks or risk analysis needs to be updated. The Group includes the following members: RAE (Coordinator) and at least one representative from the National Natural Gas System Operator and the Independent Power Transmission Operator, as well as representative of other involved parties, depending on the case.
Coordinator of the Working Group is the Risk Management Team (RMT), and has the following tasks:

- Identify risks and update their list,
- Identify the examined crisis scenarios,
- Forecast demand,
- Estimate the likelihood of occurence of scenarios,
- Simulate and estimate impacts.

2.3 Crisis Management Bodies

In order to timely declare warnings regarding an impeding state of electricity crisis, declare a state of electricity crisis as well as to manage efficiently such states of crisis, the following competent bodies are appointed:

1. **The Crisis Management Unit (CMU)**
2. **The Crisis Management Group for electricity (CMG_{ELEC})**
3. **The Coordinating Committee for Emergency Measures (CCEM)**

Structure, role and mission of the bodies mentioned above, are presented below in detail.

Crisis Management Unit (CMU)

The Crisis Management Unit (CMU) is a body of the Independent Power Transmission Operator (IPTO) and consists of members appointed by the Operator himself. Specifically, CMU consists of the following members:

1. The Director of Operation and Control of the System.
2. The following executive members of IPTO or or appointed members by the Head of CMU as vice members:
   - **a.** Director of Branch of Energy Control Centers.
   - **b.** Director of Branch of Short-term Operation Scheduling.
   - **c.** Head of Department of National Energy Control Centre.

The CMU continuously collects information about an impeding event, evaluates relevant information and received indications from every involved energy entity (DSO, power producers, HenEx, etc.), monitors the energy balance of electricity, performs continuous reassessment of the situation, cooperates closely with the RMG and the CMG, which are coordinated by RAE. In cases where serious and reliable information indicate that an

electricity crisis will occur or currently faced with an electricity crisis, CMU requests RAE to convene the CMG, the declaration of a state of crisis and its level (early warning or crisis).

After the end of the state of crisis, the CMU is responsible for collecting the final reports from energy entities which were affected from the incident which led to declaration of early warning or state of crisis, drafts the final report and submit it to RAE (RMG) with the aim to inform and update the level of risk.

Crisis Management Group for electricity (CMG_{ELEC})

The Crisis Management Team for electricity **(CMG_{ELEC})** is appointed as the competent body with the task of efficiently treating states of electricity crisis which endanger security of supply. It is coordinated by RAE, receives information and suggestions from the CMU related to the incident, and after evaluation of the severity of the event expresses its opinion regarding the declaration of the early warning or a state of electricity crisis. CMG_{ELEC} also participates in the CCEM.

A top executive member of RAE is designated as the **Head of CMG_{ELEC}**, by decision of RAE. **The Head of CMG_{ELEC} has the role of the Crisis Coordinator,** according to the Regulation. The following are participating in the CMG_{ELEC}:

1. Head of CMG_{ELEC} (representative of RAE)
2. Representative of the Ministry of Environment and Energy
3. Head of the CMU (IPTO)
4. Representative of the Transmission System Operator of the national electricity system (IPTO)
5. Representative of the Distribution System Operator (HEDNO)
6. Representative of the Transmission System Operator of the national natural gas system (DESFA)

Additionally, based on the circumstances, and the nature of the incident which can cause or is responsible for the state of electricity crisis, the Head of CMG_{ELEC} invites representatives of other involved parties. Particularly, representatives from the Data Protection Authority, the National Cybersecurity Authority and GR-CSIRT could be invited by RAE to assist the management of a state of electricity crisis, triggered by incidents of cyberattack.

The CMG_{ELEC} convenes after an invitation by the Head of the team and:

- Evaluates the incident and expresses its opinion to the head of the team, regarding the declaration of early warning or state of electricity crisis,
- Evaluates and approves the crisis response plan, including all necessary treatment measures,
- Re-evaluates the current situation and expresses its opinion in regards to the declaration of ending of the state of crisis.

Coordination Committee for Emergency Measures (CCEM)

CCEM consists of:

1. The Crisis Management Group for electricity (CMG_{ELEC})
2. The General Secretary for Civil Protection Γενική Γραμματεία Πολιτικής Προστασίας (GSCP).

The Ministry calls on CCEM to convene, upon suggestion by RAE of the Operator of HETS. Its goal is to coordinate all government services for the treatment of impacts of an electricity crisis, by taking into account the relevant directives issued by the GSCP.
Implementation of measures approved by CCEM for the Greek Territory is obligatory and is in effect after Involved, depending on the circumstances, Parties issue a relevant order.

Interactions between involved groups and entities for the management of an electricity crisis are presented in the following figure.

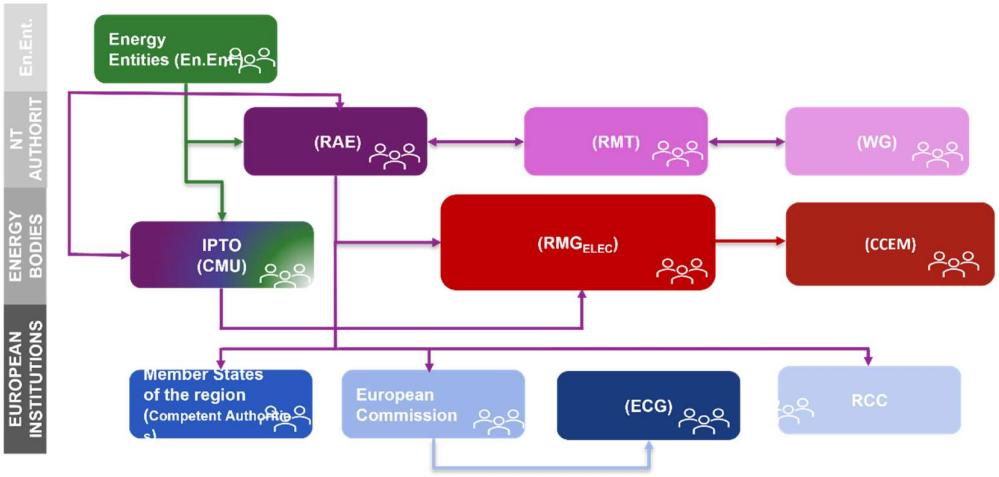

Figure 4. *Interaction between involved entities during an electricity crisis*

In conclusion, actions of all competent bodies, for as long as conditions last, based on which an early warning or a state of crisis is declared, are summarized below:

i. Instant and, in any case, timely update of the Distribution System Operator, the Operator of the national natural gas system, Power producers, Interruptible Consumers and Power Suppliers from the Head of Crisis Management Unit (CMU), as stated in the Defence Plan of HETS drawn by IPTO, through emails or any other means available, regarding the declaration of early warning or state of crisisis, and the causes which led to such a crisis. In case works or restoration actions must be carried out, information must be provided to all bodies mentioned above, regarding the duration of such actions.

ii. Communication between members and members-representatives of the system operator of CMU and representatives of Distribution System Operator and Power Producers, in order to collect all the necessary information for load forecasting, as well as availability of electricity production units to conduct a short-term adequacy study for every three (3) coming days.

iii. Provide information to the Head of CMU, within the time limit set by him, from the Distribution System Operator for electricity in regards to the possibility of load curtailment in the near future and from Interruptible Consumers in the context of their load-management contracts they have signed.

iv. Update from the Distribution System Operator for electricicty to RAE and the head of CMU, regarding the state of the Distribution System in the context of the above declaration of early warning or state of crisis, as well as existing and plannned measures to prevent and treat – mitigate impact from incidents.

v. Update RAE on a daily basis from the Transmission System Operator, regarding the progress of the incident, taken measures as well as the need for extra measures for upcoming days of the incident.

vi. Daily notifications to RAE from the Head of RMU of (a) the short-term -3 days- power adequacy study, b) unavailability of units, cause and duration of repairs and (γ) available reserves margins and possibilities for emergency imports.

vii. Under responsibility of RAE, the Ministry is informed of all the above, as well as the relevant Directorate of the European Commission.

viii. RAE requests by the competent Minister the convening of CCEM, if deemed necessary.

Finally, within one (1) month from lifting the early warning or ending the state of crisis, Operators of HETS and Distribution System Operator must submit to RAE afterwards an explanatory report, each on their respective area of responsibility, which includes at least the following:

i. Description of the event which led to the declaration of early warning or state of crisis.

ii. Description of any preventive measures, response preparedness and mitigation measures, their justification and estimation of their proportionality and effectiveness.

iii. Estimation of cross-border impacts of the measures taken·

iv. Report of the assistance which was prepared, despite being excercised or not, provided or received by neighbouring member states and third countries·

v. The economic impacts of the incident and the impacts of measures which were implemented in the electricity sector, including the cost incurred by these measures, to the extent that all available data during the estimation allow,

especially the quantities of non-served energy and the level of manual disconnection of demand (including a comparison between voluntary and forced disconnection of demand).

vi. Suggestions for the update of the Risk Preparedness Plan.

vii. Overview of potential improvements of the development of the grid, in case the insufficient development was the cause of the incident or contributed to its occurence.

2.4 National Mechanisms for Crisis Management

Mechanisms of crisis management, for the cooperation and coordination of actions and interactions between involved bodies during an electricity crisis, are presented below. In addition to groups involved in risk management and states of crisis, whose roles and responsibilities were presented above, in specific procedures, a significant number of entities, who are affected by an incident endangering the security of electricity supply, can also be involved.

Subsequently, those entities are referred as ***«Energy Entities (En.Ent.)»*** and can include:

- Producers of electricity,
- Operators of transmission and distribution electricity systems (IPTO, HEDNO),
- Operator of the national gas transmission system (DESFA) or/and
- Operators of the gas distribution system,
- The Hellenic Energy Exchange (HEnEx).

Crisis Response Team (CRG) of Energy Entities.

Each En.Ent. creates a **Crisis Response Team (CRG).** The CRG consists of individuals, responsible for the evaluation, mitigation and response to incidents, as well as individuals responsible for the evaluation of incident impacts, reporting of incidents and the communication with internal and external stakeholders.

The needs of each incident define the full size of CRG, with roles that are enabled under circumstances. In any case, each Energy Entity is responsible for defining internally the structure and roles of the specific team. Each CRG should include at least the following duties:

- Is responsible for instant response to incidents, their treatment and mitigation of their impacts,
- The Head of CRG informs without delay RAE for the occurrence of the incident,
- Cooperates closely with IPTO for the management of the incident,
- Submits a final report to IPTO, which is then notified to RAE, that includes:
    - Description of the incident that led to the electricity crisis,
    - Measures taken for the treatment and mitigation of crisis impacts,
    - Estimates the effectiveness of the above measures.

Afterwards, the roles and interactions between entities involved in risk management of electricity crisis are presented in total.

In Appendix I, in addition to the above, actions and flow of information between entities are presented in detail.

The aim of the following procedures is to notify and then take action against each incident, which can lead to a declaration of early warning or electricity crisis.

Firstly, in Figure 5, actions of RAE related to electricity crisis management are presented.

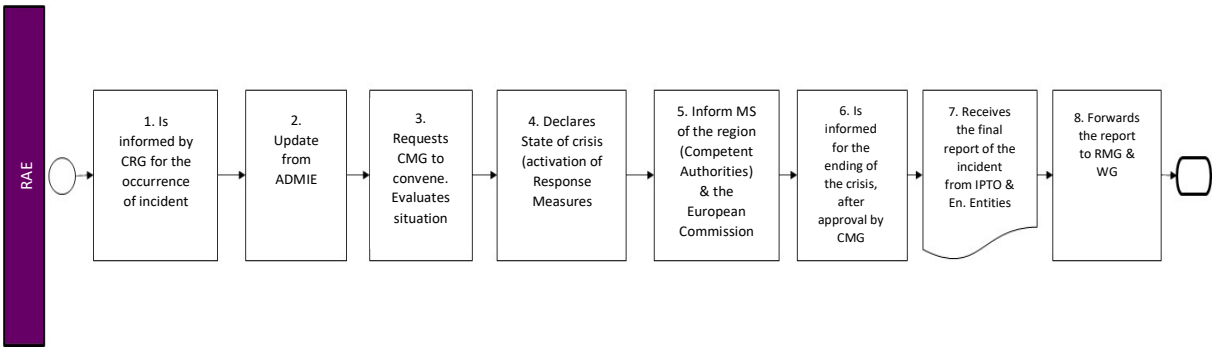

Figure 5. *Actions of RAE*

In figure 6 actions of CMG_{ELEC} are shown regarding crisis management of an electricity crisis and the flow of information between CMG_{ELEC} and involved parties.

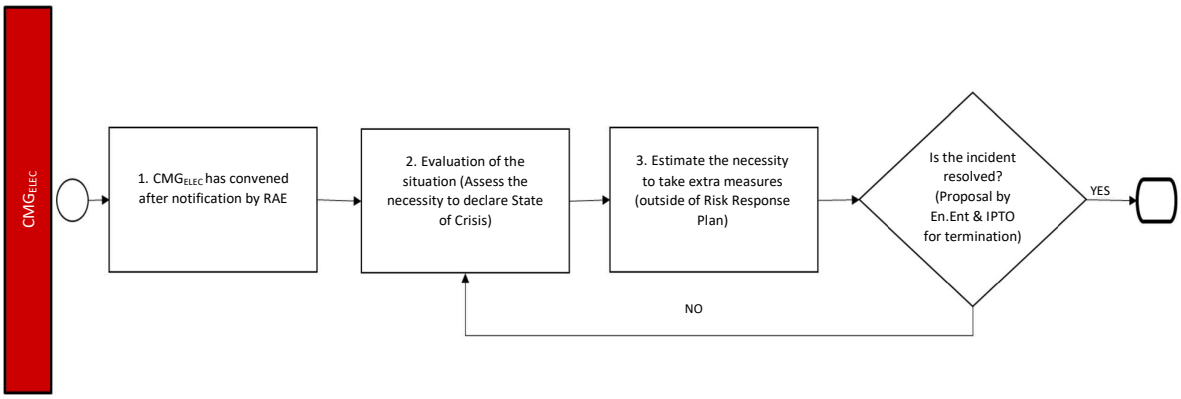

Figure 6. *Actions of Ενέργειες CMG_{ELEC}*

While in figure 7 actions of each «Energy Entity (En.Ent)» in the procedure of risk management are shown.

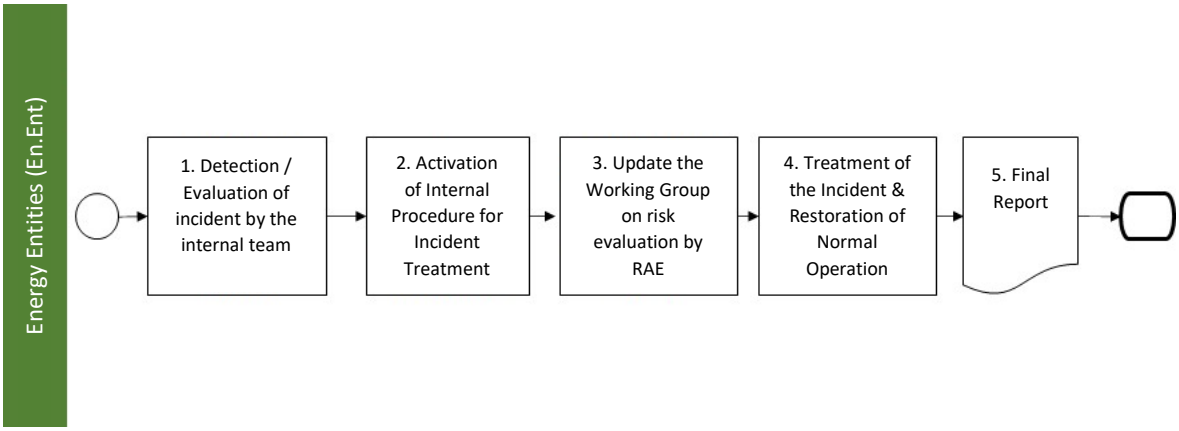

Figure 7. *Actions of Energy Entities*

Overall, actions of all involved parties for managing electricity crisis incidents are shown in figure 8.

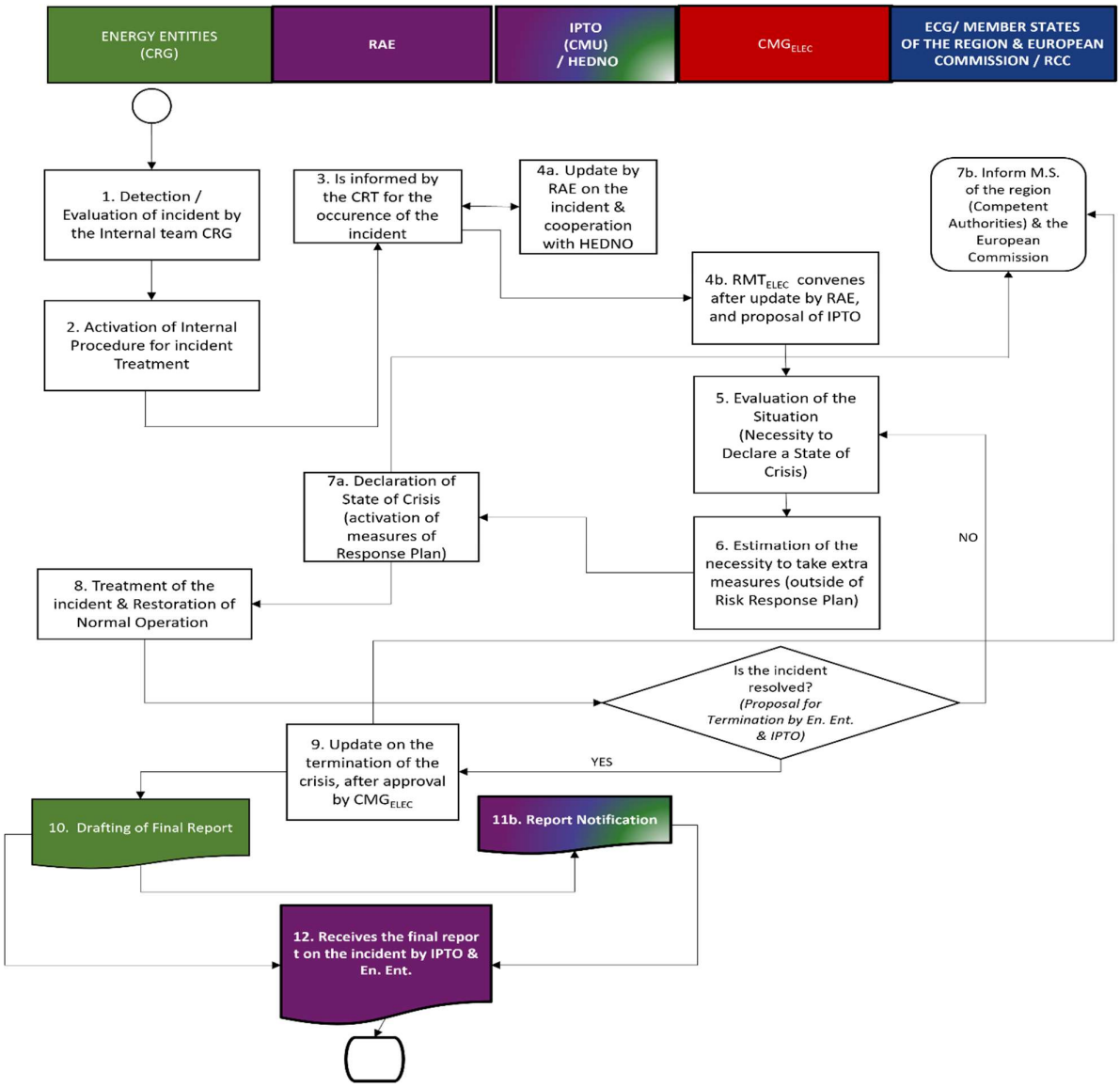

Figure 8. Schematic of the total flow of information

2.5 Electricity Crisis Management Mechanisms during incidents of cyberattacks

In cases of electricity crisis, which are caused by incidents of cyberattacks, in addition to the above, other entities with experience and responsibility of managing relevant incidents are also involved in the risk management procedure. Those are:

- The National Cybersecurity Authority
- GR-CSIRT (HNDG)
- Data Protection Authority (DPA)

Moreover, **each Energy Entity appoints a Chief Information Security Officer (ISO)**, responsible for managing incidents of cyberattacks, and has the role of Head of Entity's CR, specifically dealing with issues of cybersecurity.

The goal of the procedure presented afterwards is to enable early detection, notification and effective treatment of every cyberattack, which could endanger the security of electricity supply of the Country. Thus, each Energy Entity notifies to GR-SCIRT, the National Cybersecurity Authority and to RAE without unreasonable delay every incident which impacts continuous supply of services offered. It should be noted that reports sent to GR-CSIRT and NCA could include different information, in order to suit the needs of each Authority

The initial report is provided:

- Using email or in writing, in the form of the relevant template of NCA.
- At a reasonable time and, in any case, within 24 hours since the Organization received a notice of the incident.
- In cases, specifically, in which the incident is considered as severe disruption, the Organization is obliged to submit the initial report without unreasonable delay.

Thus, in order to manage electricity crisis caused by cyberattack incidents, the actions of Energy Entities are shown in figure 9 and the schematic of total information flow in figure 10.

In Appendix II, in addition to the above, actions and the information flow, between involved entities in electricity crisis management due to cyberattacks, are presented in detail in tables.

Figures 5 & 6 of chapter 2.4 remain as is, and apply also to cyberattacks.

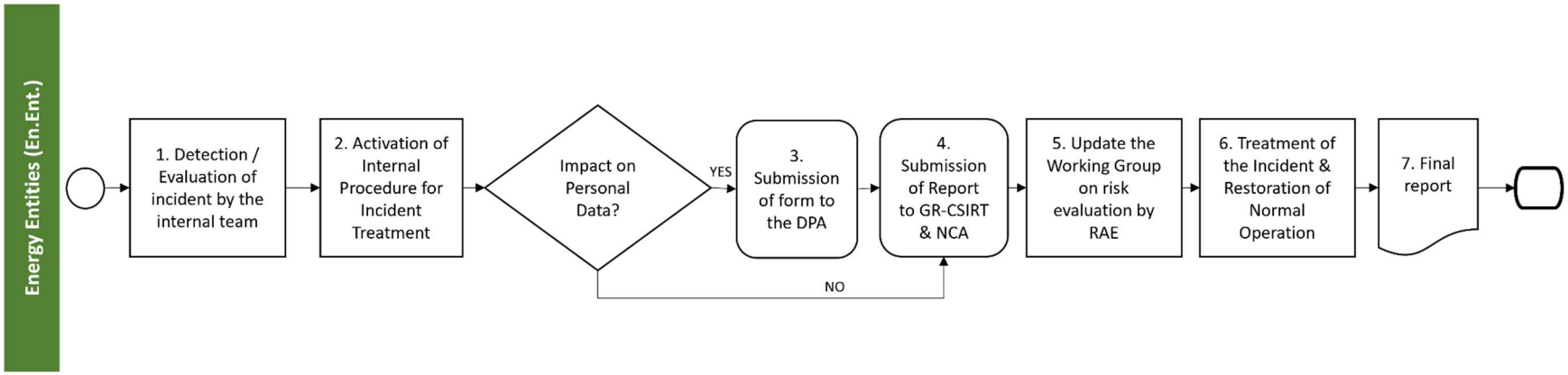

Figure 9. Actions of Energy Entities **(cyberattack incidents)**

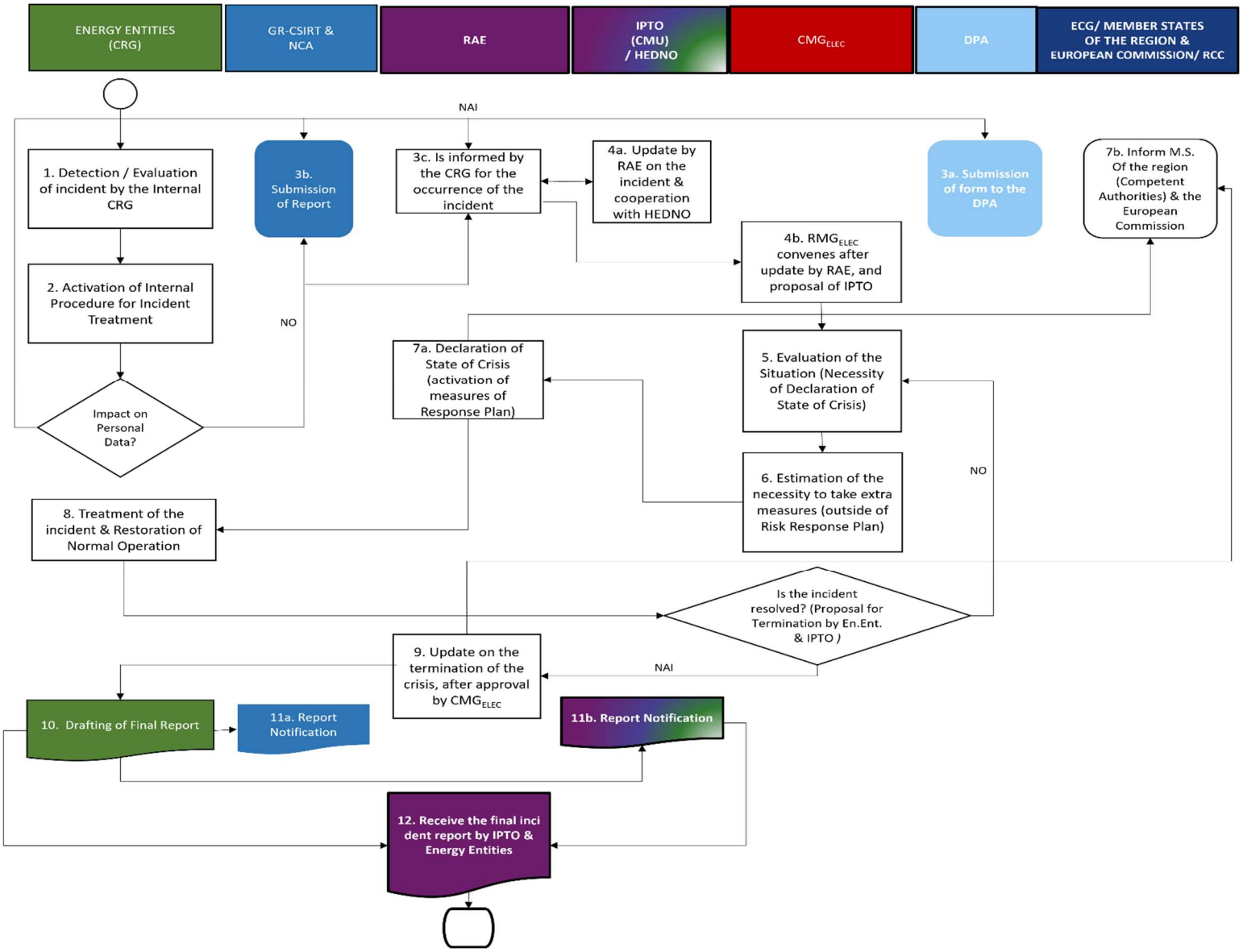

Figure 10. *Schematic of total information flow* ***(cyberattack incidents)***

2.6 Crisis Coordinator

According to provision (d) of article 11(1) Regulation (EE) 2019/941, as mentioned above, the Head of CMG_{ELEC} is appointed as the Crisis Coordinator by relevant decision of RAE.

The Crisis Coordinator calls for meeting of the CMG_{ELEC} and coordinates it, while during a crisis has the option to invite at meetings additional representatives of involved entities based on the type of incident that endangers the security of electricity.

Furthermore, depending on the opinion of CMG_{ELEC} on the incident, the coordinator informs the Board of RAE on the necessity of a declaration of early warning, state of electricity crisis or its termination.

3. Procedures and measures during an electricity crisis

3.1 National procedures and measures

In this chapter, existing national measures and measures designed in the framework of the existing Plan on prevention, preparedness and mitigation of impacts of electricity crisis are presented. Firstly, general measures implemented by the TSO (IPTO) for risk prevention and risk treatment of electricity crisis are presented, followed by targeted measures for each one of the five groups (clusters) of national risk scenarios

3.1.1 Existing measures for the operation security of the System - IPTO

Operational Planning (D-1)

The TSO is responsible for the security of the transmission system of his area of control και must comply with the requirements of Regulation (EE) 2017/1485. The first step in securing operation of the system is the Operational Planning (day D-1). Having collected all the available information regarding forecasted demand and RES production, cross-border exchange schedules, availability of units and elements of the system affecting operation, creates the operational «profile» for the next day (day D of dispatching), based on economic and security criteria. This procedure includes:

- **Enforcement of the security criterion N-1.** Scheduling and monitoring of the system is perfomed in such way, so that the loss of an important element does not affect the security of operation of the system, meaning that acceptable limits of operational security are not violated.
- **Calculate necessary reserves.** Reserves safeguard the System in cases of usual or less usual distrubances which can affect safe operating limits. The Operator has developped a methodology to calculate reserves by taking into account the characteristics of the Hellenic Electricity System and special conditions of each day. For days wth increased «stress» to the Electricity Grid, necessary reserves are also forecasted upwards. According to the «Methodology of Determination of the zonal and systemic Balancing Capacity needs (Gov. Gazette B' 3565/28.08.2020)» of the Interconnected Transmission System, while estimating system requirements for updwards/downwards mFRR, the terms $\boldsymbol{EC_{d,t}^{up}}$ και $\boldsymbol{EC_{d,t}^{dn}}$ are used respectively in order to include increased needs of the system during extreme conditions (e.g. weather conditions). The value of the aboce terms are zero during normal operation of the system, while non zero and determined accordingly based on the type and size during extreme conditions of the system.
- **Scheduling of maintenances.** During scheduling maintenances of system's elements, the main goal is to not affect negatively the security of the system (security criterion N-1).
- **Secure stability of the system.** This is achieved by using appropriate software for system state analysis, load flow analysis and dynamic stability assessment to implement preemptive corrective measures.
- **Communication and information from power plants owners** for the availability and production capability of their units.
- **Exchange of information with neighbouring TSOs.** Through continuous communication, even in real-time, for any possible incidents that can occur at a neighbouring TSO's area (extreme

weather phenomena, cyberattacks, significant equipment failure, pandemic, etc.) and can affect other neighbouring TSOs. Communication can be achieved via telephone or email.

- **Defining of technical constraints** for operational security reasons during solution of ISP schedule. The TSO takes into account possible congestions in the Transmission System, local needs for production, voltage control, etc. when solving the ISP.

State of the Electricity System according to Regulation (EU) 2017/1485.

The TSO is responsible for securing the operation of the system under specified operation security constraints, even after the occurrence of a disruption. However, when unusual and large-scale disruptions occur, this cannot be always achieved. In this case, the TSO must evaluate the state of the system, activate the appropriate alarm level and proceed with the implementation of appropriate measures. Should the occurring crisis state affect neighboring TSOs, they must be informed through procedures according to bilateral operational agreements. The states of the Electricity System are defined in Article 18 of the Regulation (EE) 2017/1485, more specifically:

- The TSO declares the **alert state** when the system operates close to operational security limits and the occurence of an unforeseen events, even after implementation of corrective measures, leads to violation of operational security limits.
- The System is in the **state of emergency** when the nominal levels of voltage, current or frequency do not meet the criteria and disconnections of equipment, loss of synchronization, supply outages lead the system to a non-secure state with increase probability of total collapse. The TSO in these cases activates one or more measures according to the system defence plan.
- The system is in the **blackout state** if more than 50% of demand is lost or voltage loss exceeds at least three minutes, which as a result triggers the restoration plan.
- The system is in the **restoration state** when the TSO, being in the emergency or blackout state, has started to activate measures of its restoration plan to restore normal operation of the System.

Measures described below refer to actions of the TSO in order to secure operation of the system, as well as restoration to normal state, and are divided into to main categories:

- **Short term measures.** Refers to measures taken close to real time and are separated in those taken before the disruption and those during or after the disruption.
- **Long term measures.** Refers to measures which will be implemented in few months or few years, with the scope of increasing robustness of the system against future extreme phenomena.

Primary set of Alarm/Emergency Actions.

For the TSO to always have a clear view of the system state, for his system as well as neighboring ones, the following are deemed necessary for the secure operation of the system:

- **Reliable Measurements.** The Energy Management System of the TSO enables monitoring, operation, study and analysis of the System. Collected information in real time (measurements and notifications in case of deviation from secure operation) ensure continuous monitoring of the system and the implementation of appropriate measures.

- **Periodical simulations.** By using the data for the topology of the system and the measurements in real time, automated simulations, analysis of unforeseen events of the system, estimation of voltage stability per 5 minutes which allow for the detection of deviations from defined operational limits, are performed.
- **Regional supervision.** In case of disruptions in neighboring TSOs, which can extend and affect the Hellenic Electricity System, the use of EAS platform **(European Awareness System)** provides information in real times of the state of all Systems of TSOs of ENTO-E, and contributes significantly in quick estimations of risks and implementation of corrective measures. Additionally, the TSO, depending on the system state and the evolution of crisis scenario, must exchange information with neighboring TSOs via email, predefined message or telepohne, regarding corrective measures which are implemented and to/not to request assistance.

Based on the level and type of impacts of a disruption, implemented measures aim to:

- ✓ restore flows of active power,
- ✓ control of voltage and active power flows, and
- ✓ reduce frequency deviations.

Power flow management. The TSO ensures that power flows, even after the occurrence of unforeseen events, will remain within secure operational limits. It also defines the time frame of temporary overloads that are allowed until the implementation of corrective measures in the case of one or more losses of significant system elements. The measures to restore normal operation of the system are the following:

- Change of the topology of the System
- Suspension of scheduled maintenances
- Operation of protective relays to isolate faults, in order to not affect a wider area of the system
- Shutdown operation of Pumped Storage Hydroelectric Power plants that operate as pumps.
- Modifications to cross-border exchange schedules with neighboring TSOs (reduce or zero exports)
- Activate reserves
- Modify active power flows of HVDC interconnection
- Start-up of additional units for increased security concerns
- Implementation of the mechanism that reduces consumption during peak hours. (Demand Response Mechanism for the participation of Dispatchable Load Portfolios in the Balancing Markets.
- Redispatching of available units
- Automated/Manual load shedding (as a last resort measure)

Management of frequency deviations. IPTO, as all TSOs operating in the Continental Europe Synchronous Area must coordinate their actions to correct in real time the Area Control Error, to satisfy frequency quality inside the synchronous area. Significant deviations appear only in cases of “islanding” of big regions. In big areas that have been isolated, huge amounts of sudden excess or lack of power are reported.

Measures taken in cases of underfrequency:

- Automatic (FCR, aFRR) or manual (mFRR) activation of appropriate upward reserves of dispatchable units within determined time frames.
- Shutdown of operations of pumping of Hydroelectric pumping units.
- Activation of additional fast start units to balance production/demand, without inflicting congestions to the Transmission System.
- Automatic load shedding mechanisms are activated in cases of high frequency deviations (as described below in detail.

Measures taken in cases of overfrequency:

- Automatic (FCR, aFRR) or manual (mFRR) activation of appropriate downward reserves of dispatchable units within determined time frames.
- Order to reduce production of power production units.
- Start up of hydroelectric pumping units in pumping operation.
- Order to desynchronize power production units.
- Automatic activation of disconnection systems of power production units.

Efficiency of production units. Significant factor for the reliability of the Transmission System is the reliability of production units. In case of major disruptions of voltage or/and frequency, units must remain synchronized after the event according to their technical capabilities. While, in case of desynchronization, they must remain operational and supply only their auxiliary loads (house-load operation). For each unit, limits of voltage and frequency have been identified, which the unit must not violate while synchronized with the system and the TSO must periodically check its compliance with the specified requirements.

Secondary set of Alarm/Emergency Actions

If the primary set of actions of TSO is insufficient to restore the System within acceptable operational limits, additional measures are activated and can impact User of the System.

Emergency Cross Border Assistance: The TSO can reduce cross border energy exchanges or request and receive emergency energy from neighboring TSOs, according to procedures and terms of the existing agreements between TSO and neighboring TSOs (Additional information is provided in chapter 3.2).

Rules for the Suspension of the Electricity Market. According to the methodology "Rules for the suspension and restoration of market activities (Gov. Gazette B' 5944/31.12.2020)", the TSO proceeds to the temporary suspension of the electricity market when operational security issues for the Electricity System appear. Such issues might be, for example, fuel supply issues of power production units or when failures to important elements of the Transmission System exist, that place the system in a state of emergency. The goal of suspension is to avoid the continuation of market activities that will either worsen the safety margins of the system during an emergency or will negatively affect the restoration procedure. This measure is implemented, provided that the TSO has exhausted all technical options available at its disposal in the context of Market Operation and has implemented all available corrective measures. During Emergency State or State of Restoration and provided that the above conditions are met for the suspension of the Electricity Market, the Integrated Scheduling Process (ISP) is not performed, and all User are obliged to follow the orders (verbal or automatic) of the TSO, provided that the safety of personnel and their equipment is not compromised.

The rules for suspension consider the percentage of load shedding, percentage of production cut-off, percentage and geographical distribution of unavailable transmission system elements so that the percentage of produced energy, which cannot be transported from one region to another within the area of TSO's control, the inability of power suppliers and balancing services, inability to use tools and means of communication for market operation.

Protection scheme of International Interconnection. International Interconnections aim to provide maximum support in case of state of emergency. However, since they are an important link with the Continental Europe synchronous area, their disconnection must a measure of last resort, in order to contain the risk of spreading the disruption in a wider geographical area. Therefore, interconnection lines with neighboring countries are equipped, in both ways, with protection relays. It is mentioned that for frequency levels of lower than 49.3 Hz the interconnection Greece - Albania is disconnected automatically, while for frequency levels lower than 48.9 Hz and 48.7 Hz that last more than 0,5 sec interconnections of Greece – North Macedonia and Greece – Bulgaria respectively is automatically disconnected from the System.

Defense Plan: A Defense Plan has been developed by IPTO in order to protect the system from large scale disruptions, according to article 11 of the Regulation (EE) 2017/2196. The Defense Plan is the last resort attempt to stabilize the system and avoid unwanted islanding of areas or even total collapse. It includes measures that are manually activated when the system is in a state of emergency and all available corrective measures are exhausted or the real-time system security analysis dictates the need to activate such measures. It also includes the following special System Protection Schemes (SPS) with automatic activation to prevent total blackout of the system:

- ✓ the automatic system for control of underfrequency load shedding (UFLS),
- ✓ the automatic system of overfrequency, which considers the ability of production units for automatic active power reduction/disconnection of production units. The TSO determines the steps of linear disconnection of production,
- ✓ the automatic prevention system of voltage collapse, which estimates load disconnection due to low voltage and measures for voltage management of the system through procedures described in the System Defence and Restoration Plan.

Load shedding

If the TSO is unable to prevent the spread of disruption and System Restoration to normal state, despite exhausting all available measures and having considered all constraints of the System, Grid and Production, it proceeds with load shedding as a last resort measure to prevent partial or total collapse of the electricity system. Load shedding is performed automatically, semi-automatically or manually, as follows:

- ➢ **Automatic load shedding.** The automatic system for control of underfrequency load shedding (UFLS) for automatic load shedding due to low frequency (different percentages of shedding for different frequency level between 49 Hz and 48 Hz). The system sends command directly to MV breakers of Grid Operator. Selection of breakers and configuration of corresponding relays is made in cooperation with the System Operator. For areas within Attica, shedded loads are grouped by regions.

- **Semi-automatic load shedding.** Refers to System Protection Schemes which include specific actions based on defined procedures performed by the Regional Control Centre (SPS of Attica and SPS of Megalopoli). Activation of those schemes is performed by the System Operator to protect specific regions in which special conditions occur that can result in voltage instability and lead to collapse. Once activated, load shedding can be performed automatically or manually from the Control Centres by sending commands directly to Transformers of Grid Operator. Special System Protection Schemes are updated each time weaknesses are detected in specific areas of the System.
- **Manual load shedding.** Is performed by orders of IPTO to the Distribution Network Operator (HEDNO), either by direct orders to customers connected to the System or to the Network. The orders are given by the Control Centre of the Network Operator via phone (or any other reliable means of communication provided it was agreed) and later on executed by the corresponding Control Centres of the Distribution Networks. (CCDN). In order to reduce inconvenience to consumers, load shedding begins from loads of lignite mines and irrigation loads. The Network Operator creates tables and prioritzes loads that will be shed (irrigation, semi-urban and finally urban loads). Additionally, it makes no distinction between consumers, determines a list of consumers with supply priority kai consumers who are not subjected to load shedding, according to the **Network Operation manual of the Management Code of the Hellenic Electricity Distribution Network**. (Gov. Gazette B' 1891/18.05.2020) (e.g. Municipalities, hospitals, security forces, army, banks, energy and communication infrastructure, transportation infrastructure, etc.)

Load shedding requires cooperation between the System Operator and the Network Operator, in the following:

- ✓ The total size of shedding is calculated by the System Operator and the Network Operator proceeds into action, according to the load priority in each region (the Network Operator begins disconnecting load based on the hierarchy, starting from low priority consumers and moving towards high priority consumers),
- ✓ The type of disconnection (manual/automatic),
- ✓ Communication with competent CCDN.

In cases where load shedding (automatic or manual) is expected to last significantly long, the procedure of **rotational load shedding** is applied. If possible, the Network Operator publicly announces the schedule of power interruption per region. Rotational load shedding is performed manually using the following ways:

- ✓ HEDNO, either on his own initiative or by orders of IPTO, είτε με δική του πρωτοβουλία είτε κατόπιν εντολής του ΑΔΜΗΕ, takes action to resupply consumers who were disconnected and proceeds with power cuts to other consumers, while maintaining the total load shedding level stable.

- ✓ IPTO sees to the rotational load shedding of customers connected directly to the System and to connection points of the System with the Network.

3.1.2 Specialized national measures for each crisis scenario

3.1.2.1 Cyberattack

Preventive measures	Impact Mitigation measures
Existing	**Existing**
• Law 4577/2018 • Ministerial Decision 1027/2019 • Law 4624/2019 • National Cybersecurity Strategy 2020-2025 • Cybersecurity Manual	• Cybersecurity Incident Response Plan
New	**New**
• *Appointment of Chief Information Security Officer (CISO)* • Appointment of Cybersecurity Team (Cybersecurity Office) • Complete Infromation Security Management System (ISMS Framework) • Continuous monitoring and analysis of incidents / Security Operations Centre • Measurement of Cybersecurity Capacity Maturity Model	• Detailed Cyber Security Incident Response Plan

Existing Preventive measures

The framework of existing preventive measures was established by adopting the relevant Regulations (EE) 2016/1148 (NIS Directive) and (EE) 2016/679 (GDPR) and incorporated in the Law.679 (GDPR). Specifically:

- National Law 4577/2018 (Gov. Gazette A' 199/03.12.2018)
- Ministerial Decision 1027/2019 (Gov. Gazette B' 3739/08.10.2019)
- National Law 4624/2019 (Gov. Gazette A' 137/29.08.2019)

Additionally, the National Cybersecurity Authority, through its actions, creates a structural framework for Cybersecurity Measures. In more detail:

National Cybersecurity Strategy 2020 - 2025

The General Directorate for Cybersecurity, following cooperation with ENISA, has already proceeded to evaluate the existing strategic planning and develops appropriate methodology for its update in the context of five (5) fundamental Strategic Objectives:

- An operational governance
- Shielding critical infrastructure, security and new technologies
- Optimization of incident management, fight against cybersecurity and protection of privacy
- A modern investment environment which promotes Research and Development

- Specifically for Objective 2 (Shielding of critical infrastructure, securite and new technologies) a special reference is made to upgrading of protection measures of critical infrastructure and to further shield them through a series of specific activities which must be implemented by obligated bodies, which include Energy Organizations, as well as Digital Service Providers (D.S.P).

Cybersecurity Manual

The Cybersecurity Manual was prepared by the National Cybersecurity Authority of the Ministry of Digital Governance, in order to provide organization of the Public Sector (as well as medium and big-sized enterprises) a set of best practices in technical and organizational protection measures based on the architecture of successive layers (also known as «defense in depth»), which are divided into a total of eighteen (18) topics. Specifically:

- Registering hardware and software
- Secure configuration of equipment and applications
- Limiting use and execution of programs and services
- Access control
- User authentication
- Network security
- Protection from malicious software
- Storing and analyzing event logs
- Security of web applications
- Remote work
- Use of cryptography
- Training and raising awareness in cybersecurity matters
- Managing risks in supply chain
- Implementing technical cybersecurity checks
- Measures of physical security of facilities
- Download security backups
- Treatment of cybersecurity incidents
- Ensure business continuity and disaster recovery

Each topic contains specialized protection measures, 183 in total, which are divided in two sub-categories, basic and improved sub-controls. Obliged bodies, to which Energy Organizations belong, it is recommended that they implement both basic and improved-subcontrols.

New Preventive Measures

In the context of improving the level of Cybersecurity of Electricity Organizations, the following preventive measures are drafted. Energy Entities are obliged to compose and send an implementation plan to the National Cybersecurity Authority and RAE. The Competent Entity for monitoring and evaluation, according to Article 9 of National Law 4577/2018 is the National Cybersecurity Authority. The results of evaluation are notified to RAE as well.

The National Cybersecurity Authority must send to RAE, at least once (1) a year a summary report for the Energy Sector with update on incident and related information.

1. **Appointment of Chief Information Security Officer (CISO) and Cybersecurity Team (Cybersecurity Office)**

Energy Entities must appoint a person with appropriate technical and organizational skills with the role of Chief Information Security Officer (CISO). The CISO is responsible for providing strategic level instructions for cybersecurity matters of the Organization, supervision and monitoring of the information security management system and ensuring compliance of the Entity with respective legislation and regulations. It is a role that requires necessary leadership characteristics and has the responsibility of coordinating the objectives of cybersecurity with business objectives of the Organization. Additionally, it plays a key role in managing cybersecurity incidents of the Organization it belongs to, as well as informing and cooperating with competent entities.

Considering the criticality as well as the complexity of Cybersecurity today, a necessary requirement for the smooth execution of the Security Plan but also addressing issues of Cybersecurity in general, is the formation of a support team in which CISO will distribute individual tasks. This team must consist of people that combine skills in Governance level and Risk Management, as well as in technical level (cybersecurity architecture, technical evaluations of systems). The number of people that are part of the Cybersecurity team is defined based on the size and needs of the Organization.

2. **Design, implementation and maintenance of a complete Information Security Management System Framework.**

The Energy Entities have to establish a complete Information Security Management System Framework, through which all technical and organizational security measures will be designed, implemented, checked, maintained and updated, as dictated by the results of Risk Management and strategic objectives of the Organization.

A common framework of Cybersecurity is expected to be specified in the context of upcoming Network Code on Cybersecurity while specific directions will be given and through the Certification Framework on Cybersecurity from ENISA, which will be common at European Union level.

Until the formal and final version of the above, the Organization can follow the internationally accepted Standards below:

- **ISO/IEC 27001**
- **NIST Cybersecurity Framework**
- **CIS Controls and Benchmarks**
- **ISA/IEC 62443**
- **NIST 800-82**
- **CSA Cloud Control Matrix (CCM)**
- Also, during the planning process of protection measures, Organization must consult the relevant **guidelines of ENISA**, such as “Power Sector Dependency on Time Service” , IoT Security, etc.

3. **Continuous monitoring and analysis of incidents through specialized Security Operations Center.**

It is one of the most critical security practices as it contributes to the early detection and response to threats in real time. The Security Operations Centre consists of advanced threat detection systems and

engineers and analysts, who monitor and investigate daily the indications of these systems. These indications come from correlations of actions on the systems of Energy Entities and may be a sign of early stages of Cyberattacks. For this reason, it is an important factor in mitigating attacks while still in an early stage.

At this point, it should be noted that due to the cost of the specific service, the ability to implement the current measure must be evaluated per Energy Entity. In any case, it would be beneficial to be implemented on all Critical Infrastructure, as identified by the Ministry of Climate Crisis & Civil Protection.

4. Measurement of Cybersecurity Capacity Maturity Model

Necessary requirement for the evaluation of the effectiveness of protection and preparation measures is the measurement of cybersecurity capacity maturity model of the Energy Organizations. In this way, an action plan is determined, with specific priority based on which the Organization will achieve the desired level of maturity. Maturity model can be defined as a set of characteristics, attributes, indicators or patterns that represent the ability and progress towards a specific sector. Maturity models usually consist of 5 level of maturity (indicatively: initial, timely definition, implementation, optimization, adaptation). Specific levels concerning Energy Entities are expected to be defined by the Network Code on Cybersecurity and published in 2022. Other models which could be used until the finalization of the above, are the CMMI (Capability Maturity model Integration), C2M2 (Cybersecurity Capability Maturity Model) και NIST ISMM (Information Security Maturity Model).

Existing Mitigation Measures

1. Cybersecurity Incident Response Plan

As mentioned in the manual on Cybersecurity, par. 17, the ability of Organizations to detect malicious attacks, respond to them and restore their operation after a breach of their system is major priority and leads to business continuity and uninterruptable service provision of the Entity. An Incident Response Plan, in order to be successful, must be characterized by the following:

- To be as detailed as possible with specific attack scenarios
- To be updated
- To be checked and simulated at regular intervals

Each Energy Organization must have drafted a Cybersecurity Incident Response Plan according to international standards (ISO\IEC 27035, NIST 800-61, MITRE ATT&CK), the directions of National Cybersecurity Authority and the Cybersecurity manual. Also, along with the plan, they must develop individual response plans to address specific scenarios. The goal of each scenario is to separate and standardize response actions per incident type as well as become the basis for testing the Incident Response Plan.

A typical Cybersecurity Incident Response Plan consists of the following phases:

Preparation: The preparation phase includes all the actions an organization must take, so as to be prepared to prevent or address an incident:

- Detailed specifications regarding Business Impact Analysis, Business Continuity Plan, Disaster Recovery Plan, according to the instructions of the Cybersecurity manual of the National Cybersecurity Authority.
- Defining roles and teams
- Identifying policies and procedures to address Cybersecurity Incidents.
- Detailed list of internal and external roles and bodies involved per case, their contact information as well as the contact person.
- Define detailed scenarios and response actions.
- Implementation of the infrastructure (hardware and software) which will be used in case of an incident, as well as the relevant locations (for example, in case staff needs to be transferred or use an alternative computer infrastructure center)

Detection and Analysis: This phase includes the detection of incident and the risk analysis based on which the criticality factor of the incident will be determined. The detection is made based on relevant security mechanisms the Organization has defined like firewalls, antivirus, SIEM, XDR, etc., as well as the Security Operations Center. Regarding the analysis, in essence it involves risk assessment of the incident (responsibility of CRG) as well as its initial report (responsibility of ISO, Information Security Officer).

Containment, Elimination and Recovery: Once the initial evaluation of the incident is made, the CRG performs containment actions of the threat so that it does not spread to other systems/regions. These actions can include isolation of a network that the attacker or malicious program is located. Having collected as much information as possible regarding the source of the threat and the affected system, CRG proceeds with all the necessary actions that eliminate the threat. Specifically:

- Indicators and causes of the incident are identified
- Safety backups are located
- Causes of the incident are removed
- The defense of the system is improved through protection measures.
- Analysis of vulnerabilities is performed
- Immediately after follows the phase of Recovery, in which the Organization must return to its normal operational level.

Specifically in the Recovery Phase:

- All operations are restored to their normal state
- The success of restoration actions is validated
- The correct operation of the systems is checked.
- Normal operational state of the systems is ensured.

Review: The last stage is the review of the incident and actions, so that an overall evaluation of the incident is made. This stage is particularly important, because its goal is to present correctly the incident to the Administration and Competent External Entities, as well as detect and correct the following points:

- Actions that, despite performed based on the plan, did not contribute substantially to the incident response.
- Actions which should have been made but were not.

- Security measures, that if existed, impact would be less severe or even nonexistent.

The report contains all minimum information, as provided for by the National Cybersecurity Authority, according to its guidelines on incident reporting.

New Mitigation Measures

Beyond the general Cybersecurity Incident Response Plan, as mentioned before, each Organization must draft a detailed plan, whose actions will differentiate based on the threat. The basic categories of cybersecurity threats are:

A. Gain unauthorized access through Advanced Persistent Threat (APT)

B. Infection with malicious software (malware/ransomware)

Γ. Distributed denial of service attack

Additionally, guidelines given by NCA and ENISA must be considered in the enrichment of the scenarios. Indicative categories ,which could complete the above ones and on a case-by-case basis they are considered subcategories of A and B, are:

- Targeted attacks on specific subsystem, as mentioned in tables of scenarios 14 (IDM, PCR, CRIDA, etc) and 15 (EMS,ACG,XBORDER,DMG)
- Attack to IT/OT
- Attack on SCADA system
- Web phising
- Remote penetration
- Deletion of Critical Productive Data

The Information Security Officer should monitor international trends and guidelines of ENISA, NCA and CSIRT, as well as being in close communication with them to renew the threat list as quick as possible.

3.1.2.2 Natural Hazards

Preventive Measures	Impact mitigation Measures
Existing	**Existing**
• IPTO is timely informed by GSCP, and is responsible for: ➢ Increased System Readiness ➢ Provision for emergency technical personnel ➢ Securing more / alternative electric paths ➢ Notification to Important Users of the Grid ➢ Cooperation with HEDNO ➢ Cooperates and notifies neighboring TSOs ➢ Checking proper operation of emergency mechanisms ➢ Action planning to reduce impacts	• IPTO implements proper corrective measures: • Managing energy flows • Voltage and reactive power flow control • Management Procedure for Voltage deviations • Issue commands to Users • Securing additional energy from available units • Limits operation of hydropumping facilities • Additional power through interconnections • Load shedding

Preventive Measures

The TSO is informed timely from the National Coordination Centre of Operations and Crisis Management regarding the emergency weather forecast of HNMS. The forecast for extreme weather phenomena is considered during the phase of operational scheduling of the system for day (synchronization of additional units, increased required reserves, tightening of safety criteria, ensuring all system components, etc.).

In case of alarm for extreme weather phenomena, the TSO implements the following preventive measures:

- **Increased system preparedness.** Provision for increased reserves and availability of equipment to address the increased chance of failure of units and important equipment of the Transmission System.
- **Provision for emergency technical personnel**. Depending on the severity of the expected phenomena, the Operator maintains in alert properly manned crews close to the regions that are estimated to be affected the most by extreme phenomena and for the duration these phenomena last.
- **Secure additonal electric paths** to supply regions that will be affected by the phenomena. Scheduled maintenances are cancelled, reoperate important elements of the system which are under maintenance, activate power production units in different areas for security reasons. Similar measures for the Network Operator.
- **Notification of important Network Users** for potential outages during normal operation, if sufficient time exists.
- **Cooperation** with the Network Operator on action coordination and defining preventive measures.
- **Communication and notification of neighboring Operators** of the evolution of phenomena and estimation of preparedness in providing assitance.
- **Proper operation checks** of the emergency mechanisms and action planning on impact mitigation.

Mitigation measures

When extreme weather events strike a big region of the system, they can deactivate important system elements through unwanted trips of breakers and lead to violation of parameters of secure operation. If not treated with proper corrective measures, there is a risk of total collapse of the system, due to successive disconnections of elements.

The existing mitigation measures are the following:

- ✓ Management of energy flows,
- ✓ Voltage control and reactive power management, as mentioned previously.
- ✓ Activation of measures, as mentioned in management procedures of frequency deviations, when deviations exceed the 200 mHz margins, while
- ✓ If frequency deviations exceed specific safety limits, the automatic mechanism is activated (overfrequency/subfrequency automatic control system).

- ✓ In cases of emergency the Operator declare the proper alarm level and proceeds with the necessary actions by issueing orders to Users.
- ✓ During the restoration process, in addition to the above actions, the Operator modifies based on his estimation the dispatching process.
- ✓ If the TSO estimates that the forecasted demand cannot be satisfied by the Dispatched Units, it secures additional energy from available units, limits operation of hydropumping storage and sees to additional power via interconnections.
- ✓ If the above actions are insufficient, load shedding takes place.

3.1.2.3 Pandemic / Human Error

Preventive measures
Existing
• Compliance with instructions of NPHO • Development of appropriate training programs for the personnel
New
• Development of Business Continuity Systems for obliged Enegy Entities • Mark projects of TYDP of IPTO with significant impact on security of supply / continuous monitoring of its implementation • Regular update of training programs

Preventive measures

Operators and owners of electricity production licenses are obliged to:

- Comply with instructions of NPHO to manage impacts of the pandemic, for example:
    - Implement work from home,
    - Spatial arrangements of internal working areas,
    - Special arrangements for workers, who belong to vulnerable groups,
    - Provide personal protective equipment, etc.
- Develop Business Continuity System which complies with specifications developed by RAE
- The regular written notification of RAE regarding the ability of the entity to address disorganizing incidents and threats and the relevant measures it develops or are implemented. The frequency of notification is defined as weekly during a crisis or every three months in any other case.
- Mark projects which are proposed in the TYDP, whose delay will impact the electricity security of supply of the country or the region.

- For marked projects it becomes mandatory to notify and provide a monitoring report, every three months from the project promoter to the Authority and submit initial GAANT chart, milestone schedules (according to the terms of production license) of the project and critical path.
    - Justification for the observed deviation in the implementation time schedule related to the last approved TYDP
    - Evaluation of the impacts of the deviation from the time schedule (on related projects, Network users, the market, security of supply of the country)
    - Documentation of measures the Operator intends to adopt in order to ensure implementation of the above projects in the new time schedule and address the impacts of their delay.

To reduce incidents of human error, mainly cases of staff that is responsible for System operation in real-time, training programs must include new information on new technologies, incident analysis at national or regional level, exchange of expertise with neighboring Operators, etc.

- **Analysis of failures:** Important events in the national or neighboring System that affect the national transmission system, are examined systematically to identify causes and impacts so that response of the system to future similar events is improved. The results of the analysis can be used to revise corrective measures and improved procedures which are activated during emergency states, for equipment relacement that did not operate properly (Relays, Circuit Breakers), for revision of bilateral agreements with other Operators.

For important events with regional impacts, Operators must send a report with description of the disruption, which led to State of Emergency, to ENTSO-E. Then, ENTSO-E publishes its own analytical study to notify all Operators.

- **Training of dispatching operators:** The continuous training of personnel responsible for the operation of the system, adressing disruptions and restoration of the system to normal operation is obligatory. Conducting training seminars, notification of the results of analysis of important failures, as well as information exchange and expertise with corresponding staff of adjacent Operators allows for improved coordination in adressing critical states of the electricity system.

The Operator has a special training room for the staff that is responsible for system operation in state of emergency, where hypothetical scenarios are simulated for the Transmission System, (Dispatcher Training Simulator - DTS). The scenarios help the staff get acquainted with possible and less possible events.

Also, exchanges between staff of Control Centers of neighboring Operators are organized, so that information on emergency response during critical operation is shared.

3.1.2.4 Fossil fuel shortage

Mitigation measures

Impact mitigation measures
Existing
• Pause operation of hydropumping units • Optimize dispatching of available units • Increase lignite stocks • Activate load reduction mechanism / Participation of Dispatchable Load Portfolios in the Balancing Market • Notification of consumers on load reduction • Activate units on cold reserve • Reduce exports to zero / emergency imports from neighboring states • Postpone unit maintenance • Activate units with fuel switching capability • Rotational power cuts
New
• Planning of compensation mechanism for power generating units with fuel switching capability for their operation during a crisis

In case existing dispatchable units and imports cannot cover the demand of the system, the following measures are implemented by IPTO:

- Pause operation of hydropumping units, if the ability to operate at full load is not reduced.
- Assess availability of all production units, and based on the available fuel reserves (lignite, natural gas, water reserves) for each day, manages their optimal operation for the security of the system.
- Increase lignite reserves (preventive)
- Activate load reduction mechanism during peak hours. (Load Reduction Mechanism that provides for participation of Dispatchable Load Portofolios in the Balancing Market).
- Activates procedures, as agreed bilaterally with neighboring states to reduce energy exports to zero and increase emergency imports from neighboring Operators who do not face power adequacy issues. (More details provided in chapter 3.2)
- Activate emergency units in cold reserve state.
- If the above measures are insufficient, it proceeds with rotational power cuts in cooperation with the Network Operator.

In cases of reduced natural gas imports through pipelines from the northern borders of the country, and thus supply issues of production units with natural gas fuel, the following measures are also implemented:

a. Postponing of scheduled unit maintenance.
b. Increased participation of lignite power plants.
c. Increased participation of hydroelectric units.

d. Request for emergency support to neighboring Operators who have no power adequacy issues.

e. Notification of consumers on reduced electricity use (mainly during peak hours).

- Reasonable management and maintenance of cooling – heating systems
- Energy saving from district lighting
- Energy saving from irrigation – drainage

f. Activation of units with fuel switching capability

- Introduction of compensation mechanism for operation of those units (as described below).

Planning of compensation mechanism for operation of units with alternative fuel

The current mechanism refers to compensation of power generation units operating with alternative fuel (diesel), during a natural gas crisis and specifically alarm state 3 of the National Natural Gas System(«Emergency Plan for Natural Gas (Gov. Gazette B' 2501/25.06.2019»).

The level of compensation depends on the time of decision of the Crisis Management Team to activate fuel switching and the subsequent order from IPTO to those units to switch to diesel fuel. Thus, the two following cases are distinguished:

1. Decision of the Crisis Management Team for operation with alternative fuel (diesel), ***after*** the submission of offers of those units to the Day Ahead Market of the Hellenic Energy Exchange (HenEnEx)
2. Decision of the Crisis Management Team for operation with alternative fuel (diesel), ***before*** the submission of offers of those units to the Day Ahead Market of the Hellenic Energy Exchange (HenEnEx)

Decision of CMG after the submission of offer in the DAM

In case IPTO orders the units to switch their fuel to diesel – following decision of the CRG – after the submission of offers in the Day Ahead Market, these units will produce electricity according to their positions in the market, fulfilling their Sell Orders until the end of the D+1 day.

A Special Compensation Mechanism for Units with Alternative Fuel is proposed. This mechanism compensates units for their operating hours with alternative fuel, and specifically from the time IPTO issued the order, up to the end of days D and D+1. Thus, the maximum duration for which a unit can be compensated cannot exceed 36 hours of operation. To calculate the exact amount of compensation, the following are considered:

(1) Revenue from the market for operation of the unit for days D and D+1, according to accepted offers of the unit on natural gas fuel. (Total Revenue from the market on natural gas fuel**)**

(2) Penalties imposed from the market due to reduced available power during operation with alternative fuel.

(3) The variable cost of production with diesel fuel (VCdi), which was used for production, for the duration between IPTO's order and the end of day D+1.

If the **total Variable Cost of production with natural gas fuel (VCng) is lower compared to the Variable cost with diesel fuel,** i.e. **VCng < VCdi**, then the sum of (1), (2) and the difference VCdi - VCng will be compensated. Hence, **the total compensation is computed as [(1) + (2) + (VCdi – VCng)].**

In cases where the VCng is equal or higher compared to the VCdi, i.e **VCng ≥ VCdi** then **the sum of (1), (2) will be compensated.**

Additionally at the same time, following the order of IPTO after the decision of CMG, the obligation to submit Sell Offers, that correspond to operation with diesel fuel (and not natural gas fuel), is imposed on all units with alternative fuel, and affects their participation on all markets (DAM, IDM, Balancing Market) for day of delivery D+2, as well as each subsequent day. This obligation remains in effect until the order is lifted by decision of CMG.

Also, the possibility of imposing an obligation to the units, so that their positions are corrected in the Intra Day Market (if applicable) on diesel fuel, is under consideration.

Decision of CMG before the submission of offer in the DAM

In case IPTO orders the units to switch to diesel fuel – following the decision of CRG – before the submission of offers in the Day Ahead Market, these units will produce electricity according to their positions in the market, fulfilling their Sell Orders in the Day Ahead and Intraday Market until the end of the day D.

The same mechanism applies, as mentioned above, with the exception that the maximum duration for which a unit can be compensated cannot exceed 24 hours of operation. The obligation imposed by IPTO to submit Sell Offers, that correspond to operation with diesel fuel (and not natural gas fuel) now refers to the day D+1.

Mechanism for the Readjustment of Bid Offers for Natural Gas.

During an alarm state 3 of National Natural Gas System, the minimization of natural gas usage and the optimization of usage of the available natural gas quantity for the purposes of electricity generation is considered imperative. Thus, it is proposed, that a mechanism is introduced, which maximizes use of units with fuel switching capability. To achieve this, an administrative mechanism must be introduced, that imposes the minimum offer price for power production units with natural gas fuel. This price reflects the scarcity price of natural gas as a resource for the Electricity System. Using this mechanism:

- the operation of units with fuel switching capability will be maximized,
- use of natural gas by other units will be reduced,
- the scarcity of fuel availability for natural gas will be reflected in the electricity market (with relevant impacts on cross-border trade),
- imposed changes to the operation of units during remaining intraday dispatching procedures and system operation will be minimized, solely due to the limitation of natural gas quantity, since the issue of NG saving will be already addressed at the stage of Day Ahead Market.

In practice, the mechanism may impose the merit order of gas-fired power plants, so that plants with fuel switching capability are prioritized, providing thus their maximum available power. Gas-fired units will be

introduced on a higher point of the merit order, satisfying more peak demand and contribute to quantity savings of natural gas within the limited availability of the resource.
Setting of the minimum price depends on many factors, and therefore it will vary, so that the real needs of the system in natural are reflected, according to the following basic parameters:

- Available natural gas quantity in the system of NNGS for electricity generation purposes for each next day of operation, according to the estimation of System Operator (DESFA). To achieve the goal of quantity saving, when the available quantity of gas is decreased, the minimum price will increase, while increased availability adjust the minimum price downwards.
- The price of diesel fuel, as it affects the variable cost of fuel of units with fuel switching. When the minimum price of offers is adjusted, it must also consider the price of diesel, so that those units are fully included in the merit order.
- Loading conditions of the system, namely the remaining demand not covered by production with absolute priority in dispatching (e.g. RES).

3.1.2.5 Failures in the Electricity system

Preventive Measures
Existing
• Relative measures are implemented, as in the cases of natural hazards and human error. Additionally, • Strict complianace with maintenance schedules • Replace old / defective equipment • Secure adequacy of spare sparts • Measures to reduce recovery time of failures

Preventive Measures

Measures, relevant to the previous risk groups, are implemented and mainly those described in the category of «natural hazards» and «human error». Failures occurring in the System cannot be predicted, however the following measures can be implemented preventively to increase the reliability of the electricity system, in the context of serving demand, maintaining quality of electricity and rapid restoration of system operation after the occurrence of disruptions.

- Strict adherence to maintenance schedules and detailed inspection of the equipment after disruptions.
- Immediate replacement of old / defected components in critical substations.
- Checks of operational effectiveness of protection devices.
- Stricter criteria during operational planning (security criterion N-2).
- Existence of sufficient equipment in warehouses and proper machines in order to reduce time of failure restorations in cases of destroyed equipment.

- In cases of failures of critical elements of the System, priority will be given to quickly fix them.
- It is important for the stability of the System, that power production units remain synchronised to the System during serious voltage or frequency fluctuations. Additionally, in cases of unit desynchronizations, such units must remain operational by supplying their secondary loads for a specific duration (house-load operation) or units with autonomous restart capabilities (black-start capability). This greatly helps quick restoration of the System.

Long-term planning

- Changes to system planning, in order to adapt to the new state of electricity production map of the country (decommissioning of lignite plants, increase RES plants, interconnection of islands, dispersed production).
- At distribution level, create more loops so that areas can be supplied through alternative paths.

3.1.3 Increase system resilience

Measures which are either during implementation phase or scheduled for the next years, according to the TYDP of Transmission System (2022-2031) of the System Operator, are briefly:

1. **Enhance security and reliability of the Transmission System.**

The System Operator, in order to increase the reliability of the System and address the impacts of climate change and sudden change of electricity energy mix, has set the strengthening of system resilience as a key priority of its strategy for the upcoming years. In this effort, several projects are implemented for the development of the System and a replacement program of old equipment with modern ones is in progress.

The replacement program includes the following:

Table 10. *Approved projects for equipment upgrade TYDP 2022-2031.*

TYDP Project Code	Project	Cost Estimation (mil. €)	Implementation Dates
20.1	Replacement of 150 kV equipment in existing S/S and HVC	6,22	2023B[3]
20.2	Replacement of 400 kV equipment in existing S/S and HVC	25,84	2023B
Subprojects of 22.1	Replacement of voltage regulation under load system in Autotransformers	4	2023B

[3] Second semester of 2023

2. Extension of the Interconnected System

The Interconnection of Mainland System with almost all islands of the Aegean is expected to be completed until 2030, providing a solution to adequacy and reliability problems they were facing for many years. Specifically, the project of the 4th Phase of Interconnection of Cyclades with the HETS is in progress, with a budget of around 470 mil. €. The project is funded with 165 εκ. € by the Recovery and Resilience Fund and is expected to be completed in 2023B. This phase includes interconnection of HETS with Serifos through Lavrio and the Interconnections of Serifos-Milos, Milos-Folegandros, Folegandros-Thira and Thira-Naksos.
Phase 2 of the Interconnection of Crete is in progress, which refers to connection of Crete (Korakia) with Attica (Paxi Megaron). The project's funding is 1 billion € and is expected to be completed in 2023B.

The Interconnection of Dodecanese is in progress, with a funding of 860 mil. € and is estimated to be completed in 2028B. The project includes the connection of HETS with Kos through Korinthos HVC, as well as interconnections of Kos-Rhodos and Rhodos-Karpathos.

The Interconnection of Northeast Aegean islands with HETS is in progress, with a funding of 1,45 billion € and is expected to be completed in 2029B. The project includes connection of Lemnos with HETS through Nea Santa HVC and Skiros through Aliveri HVC, as well as interconnections Lemnos-Lesbos, Lesbos-Chios, Chios-Samos, Samos-Kos and Lesvos-Skiros.

3. Development of International Electricity Interconnections

The new interconnection 400 kV line between Greece and Bulgaria is in progress, with a funding of 66,4 mil. €, of which 11 mil. € account for the Greek part of the project. The project is expected to be completed until the end of 2022 or beginning of 2023.

In the context of Feasibility Study for the new interconnection between Greece and Italy different technical alternative solutions are examined in detail for the development of a new submerged interconnection between the systems of Greece and Italy and the achievement of an increase in transport capacity by 500 to 1000 MW, while at the same time the possibility of using existing infrastructure of the DC Interconnection which operates since 2002 is also examined.

The project of Greece-Cyprus-Israel Interconnector refers to the interconnection of the systems of Greece – Cyprus and Israel using DC connectors and contains parts of the PCI 3.10.1 of Israel – Cyprus Interconnection and PCI 3.10.2 of Interconnection Cyprus – Greece (Crete). According to the implementing body Euroasia Interconnector, the project of electrical interconnection Greece (Crete) – Cyprus – Israel is estimated at 2,4 bil. € and completion date in 2025. The part of project PCI 3.10.2 of Cypris – Greece (Crete) Interconnection, with a funding of 1,5 bil. € has received 100 mil. € by the Recovery and Resilience Fund of the European Union through the national recovery and resilience plan of Cyprus and 657 mil. € by CEF (Connecting Europe Facility).

The upgrade of interconnection 400 kV Meliti (Greece) – Bilota (North Macedonia) has been proposed by IPTO and the Operator of North Macedonia (MEPSO). The feasibility of implementation will be examined in the next period in a joint working group of IPTO and MEPSO, which is established for this purpose.

In April 2020 a cooperation of IPTO with the Operator of the System of Albania (OST) began regarding the implementation possibility of a new interconnection Greece – Albania. Discussions are at a preliminary stage and focus on examining the technical. Economical and other parameters for the design of a new 400

kV line between the southern system of the neighboring country and a suitable High Voltage Centre in the Greek System. For this purpose, in February 2022 a joint working group was formed to evaluate all alternative possibilities.

In March 2022, IPTO and the System Operator of Turkey (TEIAS) agreed on the implementation of a new transmission line 400 kV between Greece and Turkey, with completion date in 2029. The implementation cost in Greek territory is 24,4 mil. €. (updated information on implementation dates and cost are included in the submitted TYDP 2023-2032).

In October 2021, a memorandum of cooperation between Greece and Egypt was signed, according to which a high-level working group, with the participation of representatives from both Ministries, Transmission System Operators and Regulatory Authorities, which will examine the technical and economical parameters of the Greece-Egypt Interconnector Project, will facilitate licensing and support its classification as project of European interest. In the immediate future, a joint technical committee will be established, which will include executive members of both Transmission System Operators (IPTO and EETC) for the preparation of a feasibility Study for the electricity interconnection of Greece – Egypt.

4. Integration of Storage Systems.

Utilization of existing water reservoirs of hydroelectric power plants for the construction of new pumped storage hydro plants. In existing hydroelectric plants with storage capability, new plants with pumping capability have been approved and will be constructed.
Additionally, given that the regulatory framework for storage is under development, there is increasing investment interest by market entities for the installation of battery storage systems. Furthermore. the Operator examines the potential for installation of pilot storage facilities with modern battery technology, which will be evaluated by RAE according to article 54 of the European Directive 944/2019.
In any case, the installation of storage systems will allow for optimal utilization of the dispersed RES generation, upgrade and more efficient use of transmission capacity of the system. Also, it will contribute to emergency reserves for addressing power adequacy issues of interconnected islands.

5. Upgrade transmission system stability and control.

High penetration of RES and the evolvement of the Greek Electricity System in order to achieve the goals of the National Plan for Energy and Climate, has displaced conventional production and created problems in voltage control and management of reactive power in the system, increasing substantially the needs of the system for additional compensation.

- ✓ Under responsibility of the Operator, the following projects are expected to be constructed:

Table 11. *Approved projects TYDP 2022-2031 for the upgrade of stability and control of HETS.*

TYDP project Code	Project	Cost estimation (mil. €)	Implementation dates
Subprojects of 22.1	New inductance compensation in HVC and S/S of the HETS	17,75	2024A
Subprojects of 22.1	Upgrade of information system in the National Energy Control Centre (Kryoneri)	3	2024

Subprojects of 22.1	Two (2) new dynamic compensation systems (SVC/STATCOM) at the 150 kV side of Arachthos HVC and Astros S/S (or other S/S nearby)	10	2024A

- ✓ Additionally, for stability reasons the operation of decommissioned lignite units as rotating capacitors to address the High Voltage problems is considered.
- ✓ Also, the contribution of existing RES units (wind and pv) with voltage regulation capabilities based on their production level is considered as compensation of the system.

6. **Digitalize the Transmission System** by installing advaned technology devices and use of «intelligent» technicques to mordernize the System. This ensures imporved monitoring, control and operation of the System.

7. **Creation of a single balancing market.** The System Operator contributes to the unification of balancing markets inside the European Union, as determined in Regulation (EE) 2017/2195, by participating in the creation of common european platforms for the exchange of balancing energy such as MARI, PICASSO (for the exchange of balancing energy by manual and automatic Frequency Restoration Reserves respectively) and the IGCC (for the process of Clearing Imbalances).

3.2 Regional and bilateral processes and measures

IPTO, in the context of compliance with the new Multilateral (MLA) Synchronous Area Framework Agreement (SAFA) which came into effect in April 2019, as well as the Regulations (EU) 2017/1485 and (EU) 2017/2196, has already proceeded to drafting and signing bilateral agreements regarding normal state operation as well as emergency states.

Additionally, in the context of article 6 of Regulation (EU) 2017/2196, the role of Regional Security Coordinators (RSCs) is among others to evaluate and supplement where necessary the defense plans of Operators with the process of self-evaluation at regional level.

The existing regulatory framework that defines operation of the System provides the necessary tools to address operational safety of the System.
In summary, regional and bilateral processes and measures refer to the following:

- Crisis management system at the level of communication between Crisis operators. In the framework of ENTSO-E a special list of officials from each Operator is created and maintained, so that information is transmitted safely between Operators and internally in case of a crisis,
- Annual outlooks (Winter outlook & Summer review και vice versa) in which the existing as well as forecasted and immediate upcoming state of European Systems are recorded, along with the needs and issues of the systems,
- Bilateral Operational Agreement with all neighboring Operators, which refer to actions of Operators during a crisis,
- Bilateral Emergency Agreement with all neighboring Operators. In these agreements, the necessary assistance between Operators during a crisis is described,

- Implementation of common policy (Policy 5 of SAFA) with all Operators of the Mainland European Systems during crisis and their management,
- Monitoring and operation of the European platform EAS (European Awareness System) through which the Operator is informed in real-time about the operational state of European Operators and notifies the state of its system to other Operators (article 152 of the Regulation (EE) 2017/1485),
- Participation to provisions of «Emergency Plan for Natural Gas (Gov. Gazette B' 2501/25.06.2019)», as stated in article 4 of Regulation (EE) 994/2010 of the European Parliament.

Lastly, as mentioned already IPTO has signed agreements with neighboring TSOs for providing and receiving cross-border emergency assistance, as described below.

Cross Border Emergency Assistance

The TSO can curtail cross border energy exchanges or request and receive emergency energy from neighboring TSOs, according to procedures and terms provided for in the existing agreements signed between the two parties. IPTO has signed agreements with the respective operators of Italy and Bulgaria ("Mutual Emergency Energy Delivery between IPTO and ESO-EAD" and "Mutual Emergency Assistance Service between IPTO and TERNA") where rules and conditions for emergency energy deliveries are described, without the Operator who provides assistance endangering the System in his area of responsibility and based on technical capabilities of the interconnections. Energy exchanges commence at the beginning of next hour, from which the request was submitted.

4. Consultation with interested parties

The current Plan has been sent to competent authorities of member states in the region and to ECG according to article 10, par. 4 of the Regulation.

Additionally, the draft was put to Public Consultation by RAE with interested parties from the internal energy market from 10 June 2022 to 1 July 2022. In the context of the above consultation, the following bodies submitted their remarks:

1. Elpedison S.A

RAE processed and evaluated the remarks submitted and were taken into consideration for the final submission of the Plan.

5. Emergency Tests

Emergency tests are performed every 2 years in order to evaluate the effectiveness of the Plan.
Scheduled tests and simulations of electricity crisis provide the means for evaluation of:

- Personnel (users and experts),
- Procedures,
- And Infrastructure.

It is proposed that the first Emergency Test to be performed at the third quarter of 2024.

Especially, for the evaluation of preparedness against cyberattacks, emergency tests aim at simulating real cyberattacks, which competent teams of organization must face, based on their security policies and capabilities. The goal of cybersecurity exercises is to subjectively test the procedures and capabilities of the organization. In detail, emergency tests aim at the following points:

- Training of participants in technical matters.
- Cooperation between participants at technical and procedural level.
- Distribution of techniques, ideas and procedures of incident management.
- Simulation of high level technical indidents in the scope of new technologies and realism.
- Escalation of difficulty in order for the participants to identify the level and their weaknesses by themselves.
- Possibility of training on the scenarios and excersise outside the time duration.
- Cover a broad spectrum of attack and technical incidents' types of cyberdefense - cybersecurity.

Scenarios include attacks in cyberspace at national level against infrastructure connected to the network as well as HenEx, with impact on operation, service quality, grid and final consumer protection.

The Competent Entity for coordination of testing is the National Cybersecurity Authority. The NCA, in cooperation with CSIRT, determines the final scenarios while in cooperation with RAE is responsible for scheduling the date of scenario executions.

Cyber defense exercises can be grouped into the following categories:

- Real time exercises,
- Non-real time exercises, which are performed for the evaluation of:
  - Incident handling processes of cyberattacks
  - Reporting and communication procedures (Reporting → Follow procedures)
  - Means of distribution – exchange of information
- And mixed exercises.

Appendix I

Crisis Management – Actions of involved parties and information flow

Below are presented actions of all involved parties and well as flow of information between them in the process of electricity crisis management. In chapter 2, more detailed information was given.

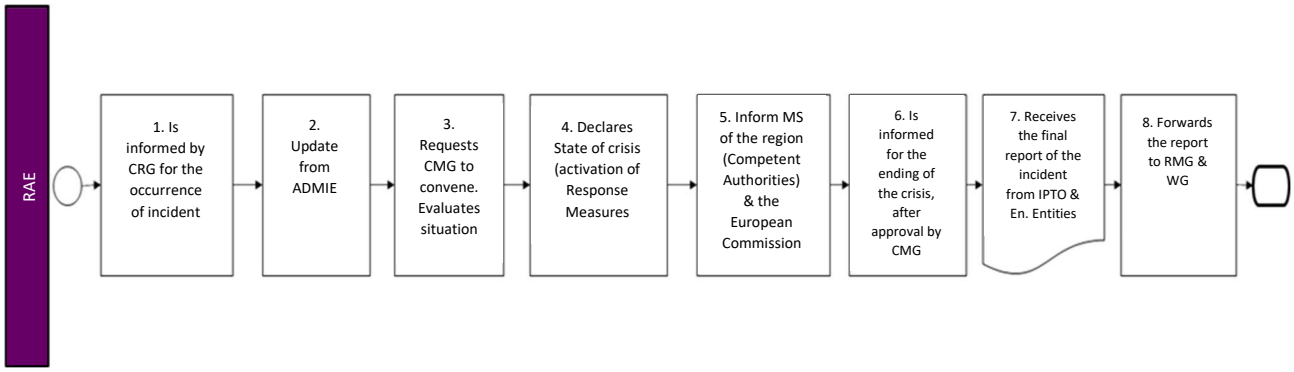

***Figure 11**. Actions of RAE*

Table 12.** Information flow & actions between RAE and involved parties in **crisis management

From	To	ACTIONS AND INFORMATION FLOW
CRG	**1. RAE**	The Energy Body in which the incident occurred, and specifically the head of CISO notifies RAE of the incident.
RAE	**2. IPTO**	RAE informs IPTO about the incident, so that it contributes to investigation / resolution if requested. **Note:** IPTO can provide information to RMG and RAE regarding expected impacts and alternative possibilities.
RAE	**3. CMG_{ELEC}**	RAE assembles and activates the CMG_{ELEC} to evaluate the situation and if necessary, declare early warning or a state of electricity crisis.
RAE	**4. RAE**	After the evaluation of the incident RAE declares state of electricity crisis or Early Warning (Activation of Measures of the Plan).
RAE	**5. E*UROPEAN INSTITUTIONS***	R*AE* notifies Member States of the region (Competent Authorities) & the European Commission on the incident. The European Commission informs in turn the ECG
CMG_{ELEC}	**6. RAE**	R*AE* is informed about the resolution of the incident (after approval of CMG_{ELEC} and proposal of IPTO) so that the end of crisis is announced.
IPTO	**7. RAE**	RAE received the final report of ADMIE and Energy Entity at least after 1 month (after the end of crisis), in which measures taken, impacts and necessity of implementation of additional measures are described.
PAE	**8.RAWG & RMG**	RAE also send the report to the Working Group for Risk Evaluation as well as to Risk Management Team in order to update the level of Risk.

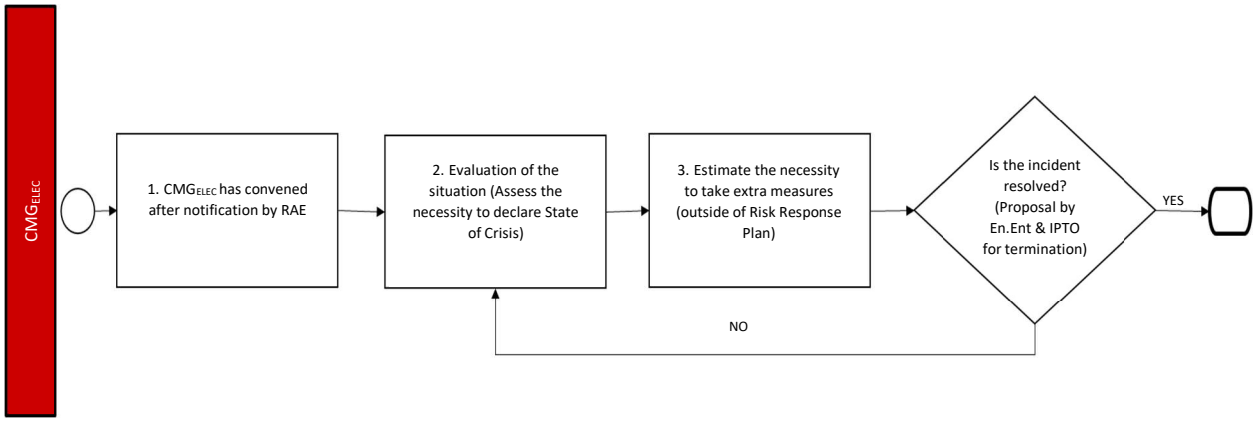

Figure 12. *Actions of CMG$_{ELEC}$*

Table 13. *Flow of information* & actions between CMG$_{ELEC}$ and involved parties in **crisis management**

From	To	***Actions and Information flow***
CMG$_{ELEC}$	**1. CMG$_{ELEC}$**	CMG$_{ELEC}$ is assembled by RAE due to occurrence of incident
CMG$_{ELEC}$	**2. CMG$_{ELEC}$**	Evaluation of the situation, and decision for the necessity of Declaration of State of Crisis
CMG$_{ELEC}$	**3. CMG$_{ELEC}$**	Estimation of Necessity of Implementation of Additional Measures
En.Ent. & IPTO	**CMG$_{ELEC}$**	Resolution of Incident? *Note: Proposal by Energy Entity & IPTO to* CMG$_{ELEC}$ *whether the incident is resolved*
CMG$_{ELEC}$	**-**	**YES** End of Procedure for CMG$_{ELEC}$.
CMG$_{ELEC}$	**5. CMG$_{ELEC}$**	**NO** Repeat step 2 and proceed with flow.

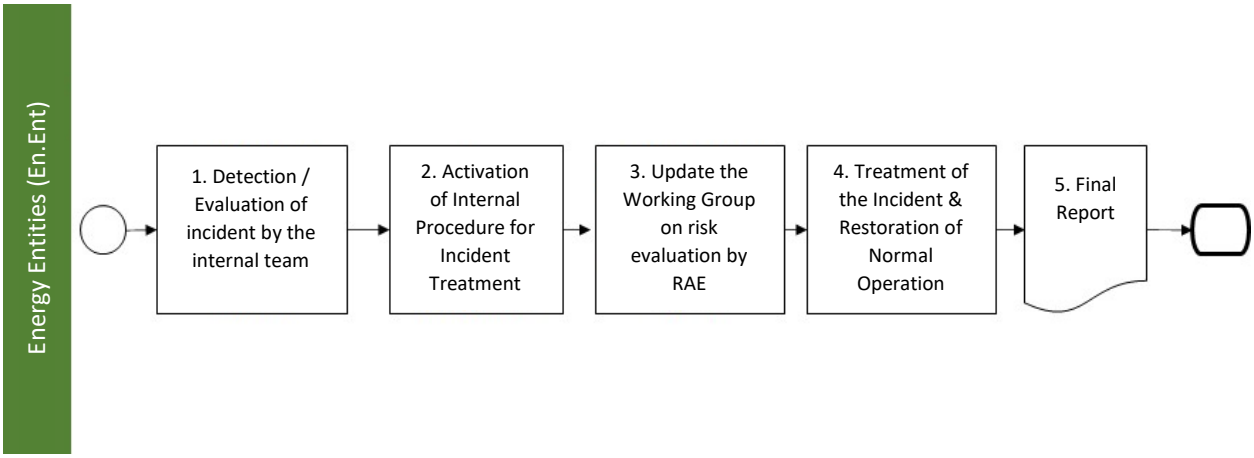

Figure 13. *Actions of Energy Entities*

Table 14. *Flow of information* & actions between Energy Entities and involved parties in crisis management

From	To	***Actions and Information flow***
Energy Entities	**1. CRG**	CRG is responsible for detection of the incident.
	2. CRG	CRG decides, according to internal procedures of each Organization, on the next actions both at the level of direct mitigation of impact and at the level of informing and coordinating with external entities.
	3. RAE	The Head of CRG sends relevant information to RAE, especially to RMG.
	4. CRG	Each CRG of affected Organization, having performed the necessary immediate actions of mitigating impact, perform additional actions in further addressing the incident and restoring operation of the systems.
	5. IPTO	IPTO receives final report / reports from each organization that was affected by the incident. Then IPTO send the report to RMG as well as to bodies of RMG in order to update the level of Risk.

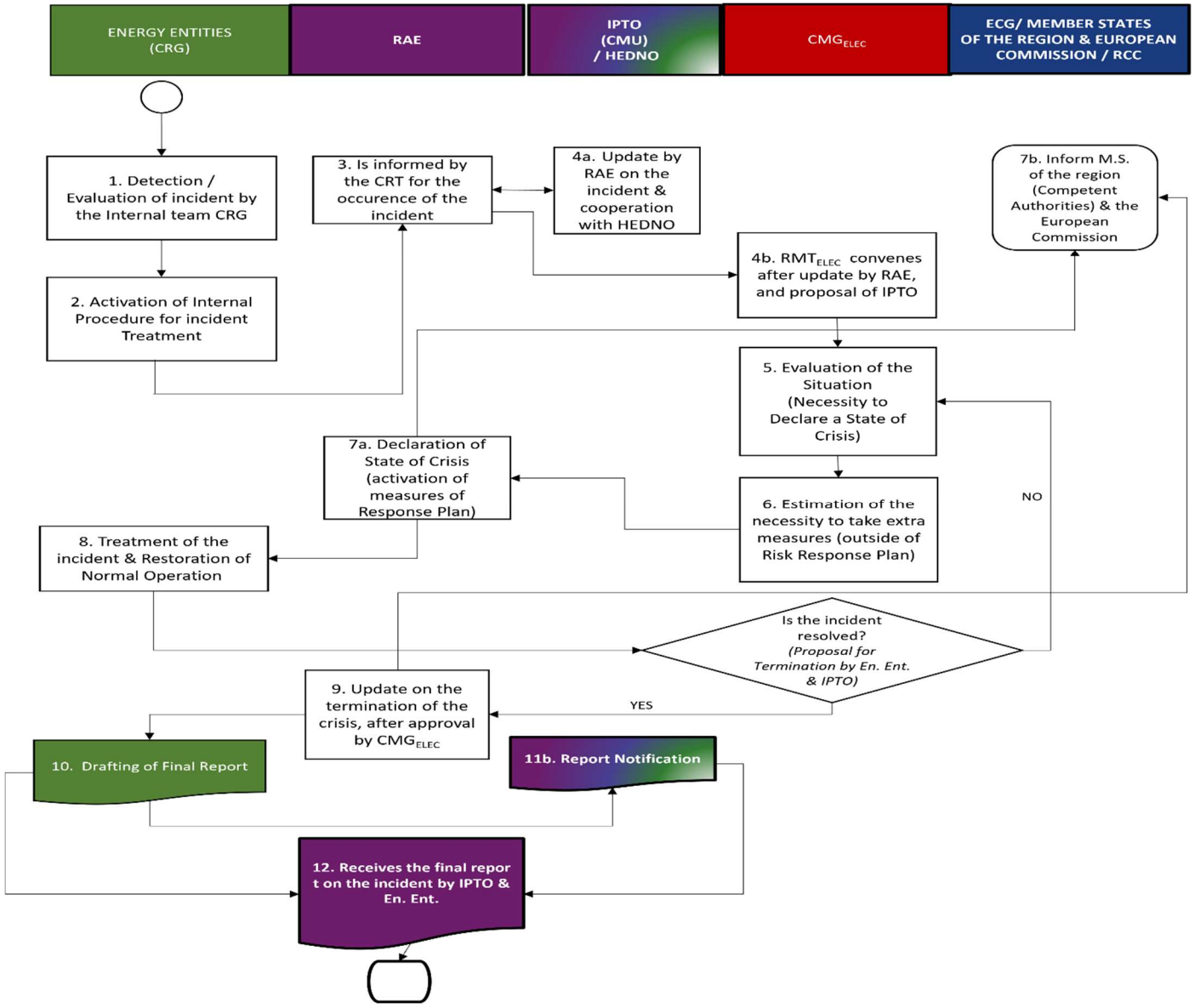

Figure 14. Schematical presentation of the total flow of information

Table 15. Total flow of information & actions between all involved parties in crisis management

From	To	***Actions & flow on information***
Energy Entity	**1. CRG**	The CRG detects and assesses the incident.
Energy Entity	**2. CRG**	The CRG decides, based on internal procedures of each Organization, on the following actions both at immediate impact mitigation level and information level and coordination with external entities.
Energy Entity	**3. RAE**	Also, the head of CRG provides information to RAE, especially RMG
RAE	**4a. IPTO**	RAE informs IPTO about the incident, so that it contributes to investigation / resolution if requested
RAE	**4b. CMG_{ELEC}**	RAE activates CMG_{ELEC} by notifying it of the occurrence of incident, together with RMG and REWG will investigate / evaluate the incident
CMG_{ELEC}	**5. CMG_{ELEC}**	Evaluation of the situation (Necessity of Declaring a State of Crisis)
CMG_{ELEC}	**6. CMG_{ELEC}**	Estimation of the Necessity to take extra Measures
CMG_{ELEC}	**7a. RAE**	RAE as a competent authority and according to article 14, paragraph 2, of Regulation EE 2019/941, after consultation with IPTO declares State of Electricity Crisis. This means immediate activation of Response Plan Measures
RAE	**7b. EUROPEAN INSTITUTIONS**	R*AE* informs Member States of the region (Competent Authorities) & the European Commission of the Incident. The European Commission in turn informs the ECG
RAE	**8.** Energy Entity	Each CRG of affected organization, having performed all necessary immediate actions to mitigate the incident, under coordination of CMG_{ELEC}, performs additional actions to address the incident and restore operation of the systems
Energy Entity & IPTO	**CMG_{ELEC}**	Is the incident resolved? ***(After proposal for Termination by Energy Entities and IPTO)***
CMG_{ELEC}	**9. RAE**	**YES** RAE declares the end of crisis
CMG_{ELEC}	**5. CMG_{ELEC}**	**NO** – Repeat step 5 Evaluation of the situation (Necessity of Declaring a State of Crisis)
CMG_{ELEC}	**Energy Entity**	The Energy Entity prepares the final report
Energy Entity	**11b. IPTO**	IPTO receives the final report / final reports from each organization affected by the incident

From	To	*Actions & flow on information*
IPTO	**12. RAE**	IPTO sends the final incident report to RAE. In turn, RAE notifies the report to the Working Group for Risk Evaluation and the bodies of RMG to update the level of Risk.

Appendix II

Electricity Crisis Management due to Cyberattacks – Actions of Energy Entities and information flow

Below, actions of Energy Entities are presented schematically as well as the flow of information between involved parties in management of electricity crisis caused by cyberattacks. Information was presented in chapter 2 in detail.

Actions of RAE and $CMG_{ELEC\ remain}$ the same as presented in Appendix I.

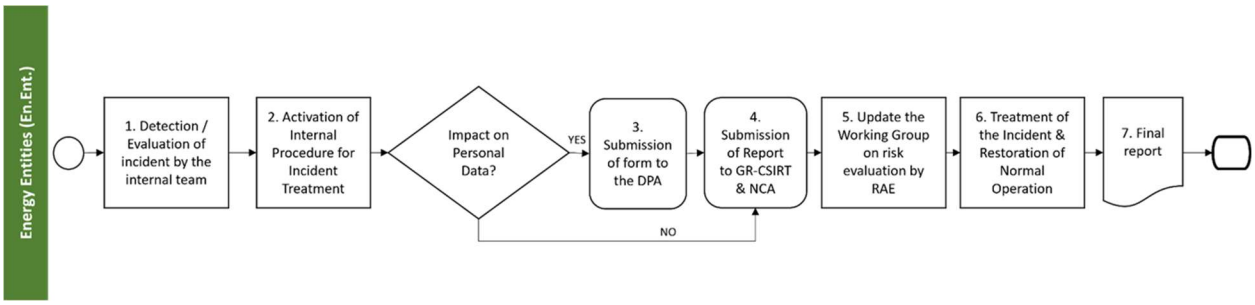

Figure 15. Actions of Energy Entity **(incidents of cyberattacks)**

Table 16. Flow of information & actions between Energy Entities and involved parties in crisis management **(incidents of cyberattacks)**

From	To	Actions & flow of information
Energy Entity	**1. CRG**	The First Response Team of CRG is responsible for the detection of the incident. This can be done automatically or communicated (internally) by an employee of the Energy Entity or relevant communication teams with external entities (customers, suppliers), which have the responsibility to inform about any cybersecurity incident. In case the incident is related to cybersecurity, it is notified immediately to the Information Security Officer
	2. CRG	CRG decides, according to internal procedures of each Organization, on the next actions both at the level of direct mitigation of impact and at the level of informing and coordinating with external entities. Responsible for the notification of the National Cybersecurity Authority, the GR-CSIRT (HNDG) and RAE is the Information Security Officer of the Organization under cyber attack
		Impact on personal data?
	3. DPA	In case the incident may risk violation of rights and personal freedoms of related people, the Organization must notify this incident to the DPA within 72 hours from the moment the responsible person for data processing is informed. The

From	To	Actions & flow of information
		information update procedure must follow the guidelines of article 63 of Legislation 4624/2019
	4. GR-CSIRT & NCA	The Information Security Officer notifies the NCA and CSIRT according to Ministerial Decision 1027/2019
	5. RAE	The Information Security Officer of CRG sends a relevant notification to RAE, especially the Working Group for Risk Evaluation of RAE
	6. CRG	Each CRG of affected organization, having performed all necessary immediate actions to mitigate the incident, under coordination of NCA, performs additional actions to address the incident and restore operation of the systems
	7. IPTO	IPTO receives the final report / final reports from each organization affected by the incident. IPTO in coordination with NCA and GR-CSIRT plan time schedules of tests regarding implementation of optimization actions that are described in the final report of each Organization. Then IPTO sends the report to the Working Group for Risk Evaluation of RAE as well as bodies of Risk Management in order to update the level of Risk

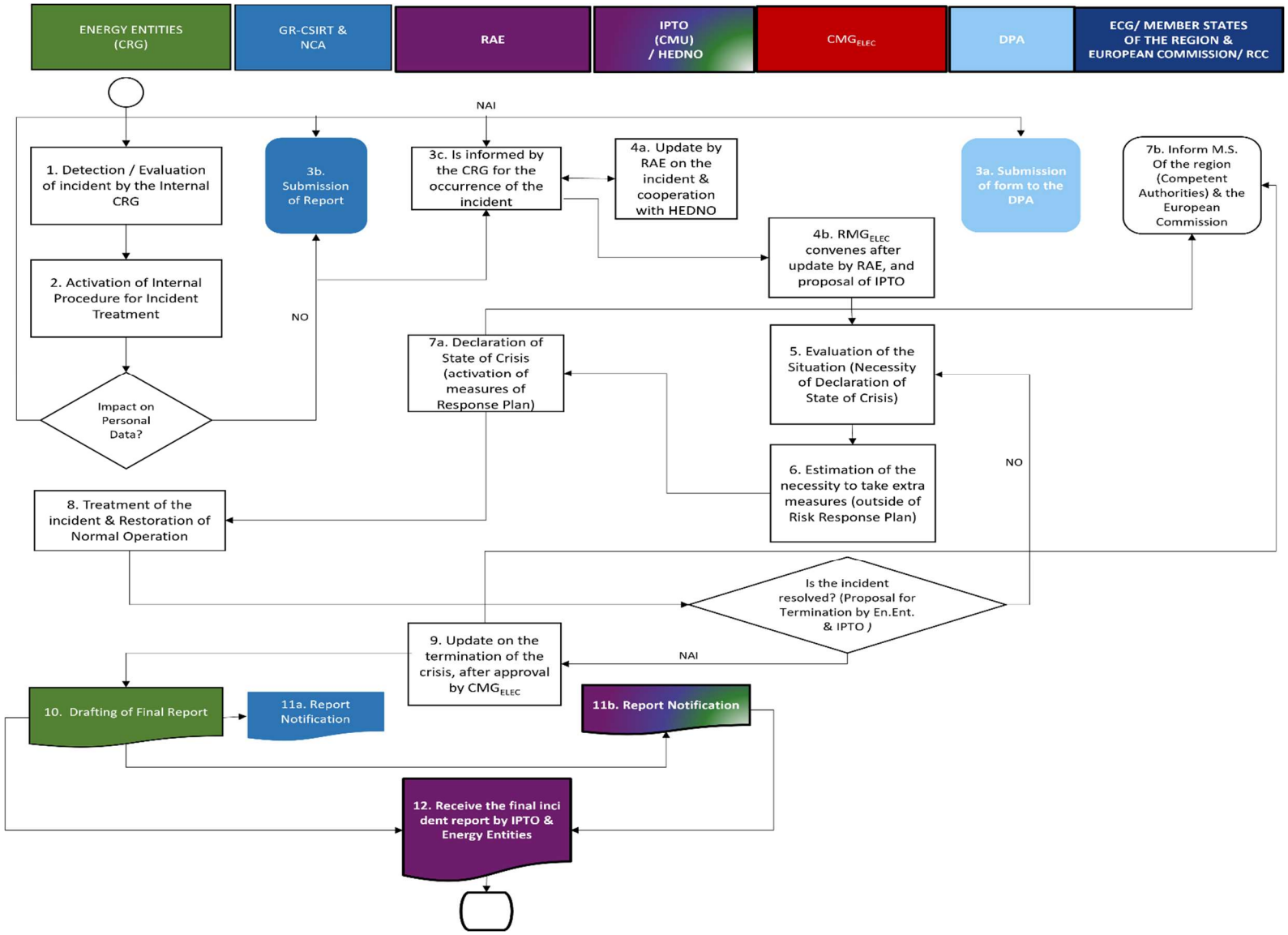

Figure 16. *Schematical presentation of the total information flow* ***(incidents of cyberattacks)***

Table 17. Total flow of information & actions between all involved parties in crisis management (**cyberattack incidents**)

From	To	Actions & Information flow
Energy Entity	**1. CRG (ISO)**	The Information Security Officer detects and assesses the incident with the help of CRG
Energy Entity	**2. CRG**	CRG decides, according to internal procedures of each Organization, on the next actions both at the level of direct mitigation of impact and at the level of informing and coordinating with external entities. Responsible for the notification of the National Cybersecurity Authority, the GR-CSIRT (HNDG) and RAE is the Information Security Officer of the Organization under cyber attack
		Impact on personal data?
Energy Entity	**3a. DPA**	**YES** In case the incident may risk violation of rights and personal freedoms of related people, the Organization must notify this incident to the DPA within 72 hours from the moment the responsible person for data processing is informed. The information update procedure must follow the guidelines of article 63 of Legislation 4624/2019 *Proceeds to step 3c*
Energy Entity	**3b. GR-CSIRT & NCA**	**OXI** The Information Security Officer (ISO) of Energy Entity informs NCA and GR-CSIRT according to Ministerial Decision 1027/2019 *Proceeds to step 3c*
Energy Entity	**3c. RAE**	Additionally, the ISO informs RAE, especially the Working Group for Risk Evaluation of RAE
RAE	**4a. IPTO**	RAE informs IPTO about the incident, so that it contributes to investigation / resolution if requested
RAE	**4b. CMG_{ELEC}**	RAE activates CMG_{ELEC} by notifying it of the occurrence of incident, together with RMG and RAWG will investigate / evaluate the incident
RAE	**4c. EUROPEAN INSTITUIONS**	R*AE,* after receiving the initial update, informs Member States of the region (Competent Authorities) & the European Commission of the Incident. The European Commission in turn informs the ECG
CMG_{ELEC}	**5. CMG_{ELEC}**	Evaluation of the situation (Necessity of Declaring a State of Crisis)
CMG_{ELEC}	**6. CMG_{ELEC}**	Estimation of the Necessity to take extra Measures (outside of the Risk Response Plan)
CMG_{ELEC}	**7. RAE**	RAE as a competent authority and according to article 14, paragraph 2, of Regulation EE 2019/941, after consultation with IPTO declares State of Electricity

From	To	Actions & Information flow
		Crisis. This means immediate activation of Response Plan Measures.
RAE	**8. Energy Entity**	Each CRG of affected organization, having performed all necessary immediate actions to mitigate the incident, under coordination of CMG_{ELEC}, performs additional actions to address the incident and restore operation of the systems.
Energy Entity & IPTO	**CMG_{ELEC}**	Is the incident resolved? ***(After proposal for Termination by Energy Entities and IPTO)***
CMG_{ELEC}	**9. RAE**	**YES** RAE declares the end of crisis
CMG_{ELEC}	**5a. CMG_{ELEC}**	**NO** – Repeat step 5a Evaluation of the situation (Necessity of Declaring a State of Crisis)
CMG_{ELEC}	**Energy Entity**	The Energy Entity prepares the final report
Energy Entity	**11a. NCA/ GR-CSIRT**	The Energy Entity in turn sends the final report – or final reports in case of more than one Entities affected from incident. ***Note:*** - *Notifies NCA, GR-CSIRT and IPTO* - *Reports are not identical, based on the needs of each Authority (e.g. more technical information provided to NCA or/and GR-CSIRT)*
Energy Entity	**11b. IPTO**	IPTO receives the final report / final reports from each organization affected by the incident. IPTO in coordination with NCA and GR-CSIRT plan time schedules of tests regarding implementation of optimization actions that are described in the final report of each Organization
IPTO	**12. RAE**	IPTO sends the final incident report to RAE. In turn, RAE notifies the report to the Working Group for Risk Evaluation and the bodies of RMG to update the level of Risk