ρυθμιστική αρχή
ενέργειας κύπρου
cyprus energy
regulatory authority

RISK-PREPAREDNESS REGULATION 2019/941

RISK-PREPAREDNESS PLAN FOR CYPRUS

September 2022

Report Reference 17/2022

Any correspondence for this document should be sent to the Cyprus Energy Regulatory Authority.

RISK-PREPAREDNESS REGULATION 2019/941

RISK-PREPAREDNESS PLAN FOR CYPRUS

Report Reference 17/2022

September 2022

Any correspondence for this document should be sent to the Cyprus Energy Regulatory Authority.

TABLE OF CONTENTS

List of Tables

EXECUTIVE SUMMARY

The scope of this document is to present the Risk Preparedness Plan for Cyprus in context of presenting the identified potential risks and crisis scenarios related to the security of electricity supply as well as to highlight the existing prevention and mitigation measures for tackling the aforementioned risks.

For the preparation of the Plan and this document, the Cyprus Energy Regulatory Authority (CERA) has collaborated with the Transmission System Operator of Cyprus (TSOC), with the contribution of the Distribution System Operator (DSO).

On the basis of the regional and national electricity crisis scenarios identified pursuant to Articles 6 and 7 of the Regulation (EU) 2019/941, the Cyprus Energy Regulatory Authority (CERA) as the competent authority, following consultation during April 2021 with relevant stakeholders as per article 10 of the Regulation (EU) 2019/941 has established a risk-preparedness plan.

In order to ensure consistency of Cyprus's risk-preparedness plan and before finalizing and adopting the Cyprus's risk-preparedness plan, CERA as the competent authority submitted on 26 May 2021 the draft plan to the ECG. It should be noted that due to the energy isolation of Cyprus there are no competent authorities of relevant or directly connected Member States, therefore the draft plan was only submitted to the Electricity Coordination Group (ECG).

In accordance with Article 13(2) of Regulation (EU) 2019/941 on risk-preparedness in the electricity sector on 7 January 2022 the European Commission has circulated among the members of the ECG the final risk preparedness plan from Cyprus for consultation. Comments were requested by 31 January 2022.

On 16 June 2022 the European Commission has formally notified the Permanent Representation its Opinion as per Regulation (EU) No 2019/941, on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, on the Risk-preparedness Plan submitted by the Competent Authority of Cyprus to the European Commission. Based on the above assessment, and in view of Article

13(c) of the Regulation, the Commission concludes that some elements of the RPP submitted by CERA do not comply with certain provisions of this Regulation.

The Commission on 16 June 2022 has also shared the notification to CERA and requested from CERA to amend the RPP taking duly into consideration all the concerns expressed by the Commission in the present opinion and notify the amended RPP to the Commission within three months of receipt of this opinion, pursuant to Article 13(3) of the Regulation. In view of the circumstances following Russia's invasion of Ukraine, the Commissions recommends to prioritise the focused update of the RPP and the detailed description of national electricity crisis scenarios described in section 2.1.1. The Commission's assessment expressed in the above said opinion is without prejudice to any position it may take vis-à-vis Cyprus as regards the compatibility of national measures with EU law, including in the context of infringement proceedings and the enforcement of European Union competition rules, including State aid rules.

CERA taking into account the Commissions' Opinion and towards the revision of the RPP, extensive discussions with all involved parties have been led by CERA.

The current Plan has been amended in order to include the missing information identified in the Opinion and fully complies with the provisions of the Regulation (EU) 2019/941.

GENERAL INFORMATION

The Cyprus Energy Regulatory Authority (CERA) is the competent authority for the preparation of the Risk Preparedness Plan.

In accordance with the preamble No. 38 of the Regulation (EU) 2019/941, Cyprus is currently the only Member State which is not directly connected to another Member State. It should be clarified with respect to certain provisions of the Regulation (EU) 2019/941, that, for as long as this situation persists, those provisions, namely provisions on the identification of regional electricity crisis scenarios, including regional and bilateral measures set out in risk-preparedness plans, and on assistance, do not apply with respect to Cyprus. Therefore, Cyprus at the time being is not required to develop any regional or bilateral procedures and measures with other Member States since in accordance with the Regulation (EU) 2019/941 Cyprus is isolated and is not part of any relevant region.

In this respect, Cyprus has developed, with the support of the Commission, alternative measures and procedures in the fields covered by those provisions, that do not affect the effective application of the Regulation (EU) 2019/941 between the other Member States.

1.1. Electricity Market in Cyprus

CERA, following a technical support project that had been carried out regarding market reorganization, concluded on the Net Pool model as being the most appropriate trading arrangement approach for the Cyprus electricity market. Based on the European Net Pool market model, all transactions of purchase and sale of electricity are conducted at a wholesale market level. Specifically, under the proposed net pool design, bilateral physical forward contracts are notified, and corresponding schedules are nominated to the Market Operator (MO) by Over-the-Counter (OTC) market gate closure on the day ahead. Suppliers and generators provide bid curves to a Day Ahead Market (DAM) on a half hourly basis. Orders in the DAM are unit based in the case of generators. Suppliers submit orders based on individually forecast demand. Orders in the DAM should correspond to quantities not already covered by bilateral contracts and take into account any Replacement Reserve of type 2 commitments. The DAM is centrally managed by an MO. The MO runs a process of matching bid curves to optimise dispatch of residual volumes at the day ahead. Contracts resulting from the DAM are between market participants and the MO at the DAM clearing price. An Integrated Scheduling Process with a real time Balancing Mechanism and later a continuous intra-day trading platform will be organized to further support market operations.

Cyprus, due its small size and limited generation portfolio, may need on a regular basis to switch-off and start up conventional units on uneconomical terms with a view to accommodating all RES output. Such an uneconomical operation of the system may have serious implications to the final tariff paid by the Cypriot consumers. To this end, it is a common procedure for curtailments of RES output (either partial or total) to take place based on overall system cost optimization during the Integrated Scheduling Process due to the small and isolated nature of the Cyprus system. This could prevent larger integration levels of RES in the island. However, the competitive electricity market model along with the introduction of appropriate processes within the Integrated Scheduling Process, would allow for RES curtailments on an economic basis with a view to minimising the total system costs, while maximizing the available RES hosting capacity.

And even though the Real-time Balancing market is not operational yet, it is expected that as soon as it is fully deployed its liquidity will increase year by year, as more products and shorter bidding deadlines are introduced. Nevertheless, to fully unlock the untapped flexibility potential on the consumer side further upgrading of the market design and the development of new digital tools and real-time communication platforms are necessary.

SUMMARY OF THE ELECTRICITY CRISIS SCENARIOS

1.2. Introduction

In accordance with Regulation (EU) 2019/941 on risk-preparedness in the electricity sector (Regulation 2019/941) Article 7, CERA, as competent authority, has identified a set of national electricity crisis scenarios as being the most relevant for the case of Cyprus. The electricity crisis scenarios were identified based on the risks referred to in Article 5(2) of the Regulation 2019/941 and in the "Methodology to Identify Regional Electricity Crisis Scenarios" of ENTSO-E, and are consistent with the regional electricity crisis scenarios identified in accordance with Article 6(1).

In identifying the Cyprus' electricity crisis scenarios, CERA consulted the Transmission System Operator of Cyprus (TSOC) and the relevant producers through their trade bodies.

On 22 December 2020, CERA, by Decision 432/2020, published the report "Identification of National Electricity Crisis Scenarios for Cyprus" on its website and informed the Electricity Coordination Group (ECG) and the European Commission about the publication, in accordance with the provisions of Regulation 2019/941. The report "Identification of National Electricity Crisis Scenarios for Cyprus" is attached to this report as Annex.

1.3. Definition of electricity crisis

Electricity crisis refers to any situation that presents a significant disruption to the supply of electricity to final consumers. More specifically, a National Electricity Crisis is a national event of energy resource inadequacy or incapacity to supply final electricity customers that could lead to declaration of Early Warning or Emergency.

According to the definition in the Transmission and Distribution Rules, which are the network code applicable to the isolated system of Cyprus, a crisis can be any abnormal situation requiring automatic or immediate operations to prevent or minimise the disconnection of transmission system or generation assets, which would negatively affect the ability of the system to serve its customers. Such cases include, but are not limited to:

- The presence of serious problems in the operation of the transmission and/or distribution system
- Partial or total black-out
- Expectation of lack of adequacy
- The safety of the system, people or equipment being jeopardised

CERA, as the competent authority for the application of the Risk Preparedness Regulation, uses the following additional criteria in its interpretation of the definition of an electricity crisis:

- Violation of N-1 standard or/and
- Expected Energy not Served (EENS) ≥ 0,001 (% of annual demand) or Loss of Load Expectation (LOLE) ≥ 3 hours/year or/and
- Cyberattack incident that will lead to economic impacts due to a disruption to the electricity system and/or the electricity market

1.4. Identification of National Electricity Crisis Scenarios

The following table presents a summary of the electricity crisis scenarios identified as relevant for Cyprus, categorised based on the following risks: (a) rare and extreme natural hazards; (b) accidental hazards going beyond the N-1 security criterion and exceptional contingencies; (c) consequential hazards including the consequences of malicious attacks and of fuel shortages.

Table 1: Cyprus' electricity crisis scenarios

Initiating event	Crisis Scenario	Based on ENTSOE	Name
Consequential hazards including the consequences of malicious attacks and of fuel shortages.	1	1	Cyberattack – entities connected to electrical grid
	2	3	Physical attack – critical assets
	3	4	Physical attack – control centres
	4	5	Threat to key employees
	5	6	Insider attack
	8	13	Fossil Fuel Shortage
	16	23	Strike, riots, industrial action
	17	24	Industrial/nuclear accident
	18	26	Unusually big RES forecast errors

	19	27	Pandemic
Accidental hazards going beyond the N-1 security criterion and exceptional contingencies	9	15	Local technical failure
	11	17	Loss of ICT systems for real-time operation
	12	18	Simultaneous multiple failures
	13	19	Power system control mechanism complexity
	14	20	Human error
	15	22	Serial equipment failure
Rare and extreme natural hazards	6	11	Precipitation and flooding
	7	12	Winter Incident
	10	16	Multiple failures caused by extreme weather
	20	28	Heatwave
	21	30	Earthquake
	22	31	Forest fire

Each scenario was rated according to its likelihood of occurrence and its consequences, should it occur. For the classification of the likelihood and the impact of each crisis scenario, the crisis likelihood and crisis impact scales of the "Methodology to Identify Regional Electricity Crisis Scenarios" of ENTSO-E were used. The overall rating for each crisis scenario was obtained by combining the estimated scenario likelihood and scenario impact, in line with the above methodology. Table 2 presents the crisis likelihood scale, Table 3 the crisis impact scale, and Table 4 the combined scenario rating scale. The rating for each of the identified electricity crisis scenarios fof Cyprus is shown in Table 5.

Table 2: Crisis likelihood scale[1]

Classification	Events per year	1 x in ... years	Description/example of initiating event
Very likely	≥ 0.5	2 or less	event expected practically every year, e.g. winds/storms causing multiple failures of overhead lines may be expected nearly every year in some areas
Likely	0.2-0.5	2-5	event expected once in a couple of years, e.g. heat wave causing limits on output of open-loop water-cooled power plants, low water levels at hydro plants, higher load, etc.
Possible	0.1-0.2	5-10	event expected or taken into consideration as a potential threat, e.g. cyber or malicious attack
Unlikely	0.01-0.1	10-100	very rare event, e.g. simultaneous floods causing unavailability of generation, distribution and transmission infrastructure
Very unlikely	≤ 0.01	100 or more	event irrelevant, or extremely rare, e.g. earthquake causing a huge destruction of transmission, distribution and generation infrastructure

Table 3: Crisis impact scale[2]

Classification	EENS% (of annual demand)	LOLE [hours]
Disastrous	≥0,25%	≥168
Critical	≥0,05% and <0,025%	≥48 and <168
Major	≥0,01% and <0,05%	≥12 and <48
Minor	≥0,002% and <0,01%	≥3 and <12
Insignificant	<0,002%	<3

[1] Methodology to Identify Regional Electricity Crisis Scenarios in accordance with Article 5 of the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC

[2] Methodology to Identify Regional Electricity Crisis Scenarios in accordance with Article 5 of the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC

Table 4: Crisis scenario rating[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

Table 5: Cyprus' electricity crisis scenarios likelihood of occurrence

Crisis Scenario	Name	Impact		Likelihood	Rating
		EENS/%	LOLE		
1	Cyberattack – entities connected to electrical grid	Critical	Major	Possible	Major
2	Physical attack – critical assets	Disastrous	Disastrous	Possible	Critical
3	Physical attack – control centres	Critical	Major	Possible	Major
4	Threat to key employees	Critical	Major	Possible	Major
5	Insider attack	Critical	Minor	Possible	Major
6	Precipitation and flooding	Minor	Minor	Likely	Minor
7	Winter Incident	Critical	Major	Likely	Critical
8	Fossil Fuel	Disastrous	Disastrous	Possible	Critical

[3] Methodology to Identify Regional Electricity Crisis Scenarios in accordance with Article 5 of the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC

	Shortage				
9	Local technical failure	Disastrous	Disastrous	Possible	Critical
10	Multiple failures caused by extreme weather	Critical	Minor	Unlikely	Minor
11	Loss of ICT systems for real-time operation	Critical	Major	Possible	Major
12	Simultaneous multiple failures	Critical	Minor	Unlikely	Minor
13	Power system control mechanism complexity	Critical	Minor	Unlikely	Minor
14	Human error	Critical	Minor	Possible	Major
15	Serial equipment failure	Critical	Minor	Possible	Major
16	Strike, riots, industrial action	Critical	Major	Unlikely	Minor
17	Industrial/nuclear accident	Disastrous	Disastrous	Possible	Critical
18	Unusually big RES forecast errors	Insignificant	Insignificant	Unlikely	Insignificant
19	Pandemic	Major	Major	Possible	Major
20	Heatwave	Major	Critical	Very likely	Critical
21	Earthquake	Disastrous	Disastrous	Very unlikely	Minor
22	Forest fire	Minor	Critical	Likely	Major

Several assumptions have been made in relation to the conditions in which the Crisis Scenarios are realized. The assumptions considered a "worst case outcome" where the duration, the ENS as well as their respective ratings based on the ENTSO-E methodology have been determined. The following table summarizes a mapping between the Crisis Scenarios along with the identified quantitative metrics.

Table 6: Quantitative analysis of the Crisis Scenarios

Scenario	Description	Worst Case Outcome	Duration/ hours	ENS/ MWh	ENS/ % annual demand	ENTSO-E Duration Rating	ENTSO-E ENS Rating
1	Cyberattack - entities connected to the electrical grid	Black out, with delayed recovery (SCADA corrupted/unavailable).	18	9522	0,1869%	Major	Critical
2	Physical attack - critical assets	Black out with long lasting lack of generation adequacy	1488	411797	8,0809%	Disastrous	Disastrous
3	Physical attack - control centres	Black out with recovery without SCADA (eg. Tripped Loads that lead to Overvoltages).	18	9522	0,1869%	Major	Critical
4	Threat to key employees	Black out with recovery via the emergency control room - Assuming that that no infrastructure is destroyed.	12	6756	0,1326%	Major	Critical
5	Insider attack	Black out with normal recovery - Assuming that the employee is detected and their access to critical infrastructure is revoked, and that no infrastructure is destroyed.	6	3598	0,0706%	Minor	Critical
6	Precipitation and flooding	Although we said in the scenario description that the worst case possible outcome is black out (worst case impact is a localised flash flooding of a city substation, with recovery equal to the time needed for the DSO to switch to feed loads from alternative Substations).	5	121	0,0024%	Minor	Minor
7	Winter incident	The worst case is considered to be a small tornado in the area of Vasilikos which damages all the transmission lines leaving the power station, thus causing a black out.	24	9513	0,1867%	Major	Critical
8	Fossil fuel shortage	Cyclic load shedding due to fuel shortage.	647	98626	1,9354%	Disastrous	Disastrous
9	Local technical failure	Loss of a key substation	744	112845	2,2144%	Disastrous	Disastrous
10	Multiple failures caused by extreme weather	Blackout with normal recovery	6	2994	0,0588%	Minor	Critical

11	Loss of ICT systems for real-time operation	Blackout with recovery without SCADA	18	9522	0,1869%	Major	Critical
12	Simultaneous multiple failures	Blackout with normal recovery	6	3598	0,0706%	Minor	Critical
13	Power system control mechanism complexity	Cascading failure leading to black-out, with normal recovery	6	3598	0,0706%	Minor	Critical
14	Human error	Black-out with normal recovery	6	3598	0,0706%	Minor	Critical
15	Serial equipment failure	Black-out with normal recovery	6	3598	0,0706%	Minor	Critical
16	Strike, riots, industrial action	Cyclic load shedding due to a long lasting strike.	47	7198	0,1413%	Major	Critical
17	Industrial/nuclear accident	Destruction of Vasilikos Power Station due to an explosion	1488	411797	8,0809%	Disastrous	Disastrous
18	Unusually big RES forecast errors	Interruption of MV feeders, either to reduce load due to a temporary shortage of generation, or to curtail reverse power flow to the transmission system due to temporary excess generation.	0,5	50	0,0010%	Insignificant	Insignificant
19	Pandemic	Temporary cyclic load shedding due to limited availability of staff (to operate units and/or to repair faults).	14	932	0,0183%	Major	Major
20	Heatwave	Cyclic load shedding due to high demand and many unplanned outages.	50	750	0,0147%	Critical	Major
21	Earthquake	Cyclic load shedding due to destruction of Vasilikos Power Station.	1488	411797	8,0809%	Disastrous	Disastrous
22	Forest fire	Temporary loss of power to Troodos due to damage of the Troodos line.	48	491	0,0096%	Critical	Minor

1.5. Summary of National Electricity Crisis Scenarios

Crisis Scenario 1: Cyberattack – entities connected to electrical grid

This scenario could be initiated at any time by an attack against critical ICT systems of TSOC, EAC, major RES producers and major consumers. The attack could cause unintended outages of lines, transformers, power plants, etc. with possible overloading on remaining lines and transformers and/or direct loss of supply. Due to the small and isolated nature of the system, a successful intrusion into a single power station or disconnection of critical transmission equipment could lead to a black-out. Furthermore, the attack could limit the TSO's ability to react to the situation due to the SCADA becoming unavailable and/or corrupted.

Crisis Scenario 2: Physical attack – critical assets

This scenario could be initiated at any time by a physical attack against power lines, transformers, substations, power plants or data centres. Electricity generation and/or transport is in danger, potentially resulting in loss of load, loss of part of the system and even a black-out, particularly in case key substations are destroyed. Violations of the N-1 security criterion and/or inability to supply some load may be long lasting, depending on the destroyed assets and the time required to restore them. Furthermore, due to the small and isolated nature of the system, a successful attack on a major power station could lead to a severe and long-lasting lack of adequacy.

Crisis Scenario 3 – Physical attack – control centres

This scenario could be initiated at any time by a physical attack on control centres of TSOC or major EAC power plants. The TSO and/or power plant operators are no longer able to monitor or control the grid/power plants. Electricity transport and delivery are still possible, but in case any actions are needed to react on incidents, the security of supply will be in danger and possibly interrupted, with even a blackout being a possibility, due to the small and isolated nature of the system.

Crisis Scenario 4 – Threat to key employees

This scenario could be initiated at any time by critical personnel who are forced to perform system destabilizing actions. The attacked or threatened employee could create multiple faults on the transmission system, damage infrastructure elements, and even shut down the whole grid thus causing a blackout.

Crisis Scenario 5 – Insider attack

The scenario would be initiated through sabotage by employee(s) or subcontractor(s) via physical intervention or misuse of ICT systems. The insider could create multiple faults on the transmission system, damage infrastructure elements, and even shut down the grid thus causing a blackout.

Crisis Scenario 6 – Precipitation and flooding

The scenario is initiated by the rainfall equivalent of weeks or months falling in the space of minutes or hours, causing localised flooding that affects substations and/or power stations. The scenario can result in flooding of substations, as well as difficulties to travel for personnel, inducing a higher response time. There could be unexpected loss of load in the areas where the flooding is high enough to damage generation and/or transmission and/or distribution infrastructure. In case of single point generation, a blackout is also possible.

Crisis Scenario 7 – Winter Incident

The scenario is relevant during the winter period. Demand is likely to be high due to low temperatures. The scenario is initiated by strong winds and/or intense lightning activity disrupting power supply and/or damaging transmission lines. Faulted conductors and towers could cause loss of load, fragmentation of the network and possible islanding. If key substations are knocked out of service, a black-out is also possible. Fault repair times could be longer than normal due to the storm.

Crisis Scenario 8 – Fossil Fuel Shortage (updated in line with recent developments due to the war in Ukraine)

The scenario is triggered due to external events (eg. Political/economic) leading to a disruption in international oil markets and/or shipping routes. There could be forced supply curtailments (selected areas/entities/hours) and an increased risk of load shedding that would result both from fossil power plant shutdowns and from curtailing renewable generation. Beyond the impacts to the supply of electricity, fuel shortages could also be very disruptive to many sectors of the economy which directly use fossil fuels as inputs, such as transportation and construction. However, it is not expected that there would be any significant switch from other energy sources (eg. heating oil) to electricity.

Cyprus does not use natural gas in any sector of the economy, and as such it is not directly affected by shortages in the supply of natural gas. However, a severe shortage of natural gas in Europe is expected to put a stress on the supply of heavy fuel oil and diesel oil, which are used in electricity generation in Cyprus, as countries affected by the gas shortage switch to alternative fuels. This can have widespread impacts on the economy, due to the increased costs to procure fuels and thus to produce electricity. Furthermore, the increased pressure in international oil markets may create difficulties in obtaining oil of the appropriate specifications, which could in turn increase the likelihood of generation unit faults if inferior quality oil is used. Delays in shipments are also possible. In a worst case scenario, a pronounced switch of natural gas consuming countries to oil could lead to shortages in international oil markets, thus triggering an electricity crisis in Cyprus.

Although this scenario is not considered to have a high likelihood of occurrence, its materialisation would have a major impact as Cyprus has limited RES generation and no endogenous fossil energy sources nor cross-border trading, thus it relies for around 85% of its electricity generation on fossil fuel imports.

Crisis Scenario 9 – Local technical failure

This scenario could occur at any time. The initiating event may be a local technical failure of key transmission infrastructure and could lead to failure of critical elements (e.g. substation), due to e.g. fires inside a substation or an explosion inside a substation. There could be system instability as well as a risk of partial blackout.

Crisis Scenario 10 – Multiple failures caused by extreme weather

The initiating event may involve multiple failures caused by the extreme weather situation. As such, it is more likely to occur in the winter or summer. For example, multiple network components of the same type start failing unexpectedly due to a heat wave in a short period of time, or multiple transmission lines fail at the same time due to strong winds. There could be a limitation or total loss of availability of ancillary services, loss of critical grid elements, possible cascading effects and system instability as well as a risk of blackout.

Crisis Scenario 11 – Loss of ICT systems for real-time operation

The initiating event can occur at any time due to technical failures resulting in the unavailability of a substantial part of the telecommunication infrastructure or one or more ICT systems used for power system in real-time planning and operation. There could be a possible use of forced (but controlled) disconnection as a remedial measure or a possible emergency disconnection of some demand or supply. In a worst-case scenario, a cascading event may be triggered. An emergency disconnection (especially a blackout) will result in potential other damages outside the electricity system.

Crisis Scenario 12 – Simultaneous multiple failures

The scenario is initiated by multiple grid elements failing at the same time (or very close together) independently of one another, resulting in N-1 security violation, and is more likely during bad winter weather. Examples include:

- multiple generators tripping in close succession,

- failures at substations or transmission lines,
- N-1 violations not being detected due to inaccurate or incomplete modelling,
- N-1 violations not being detected due to metering or monitoring failure,
- a security standard violation due to operational error or control reaction not being fast enough.

There could be a shortage of electricity as well as frequency response being held on the system resulting in low frequency demand disconnection. Operational parameters (e.g. voltage, active power) could go beyond operational security limits, and in extreme cases it can lead to a blackout.

Crisis Scenario 13 – Power system control mechanism complexity

The scenario may be initiated at any time by technical failures on IT systems, communication systems or grid protection components, resulting in a cascade failure. This would be a result of high interdependencies in very complex systems. The supply could be limited due to cascading event, with even a blackout being a possibility.

Crisis Scenario 14 – Human error

The initiating event may be a mistake of the operator or service staff, leading to a cascading event due to human error. This is more likely to occur either during maintenance, which normally takes place during spring and autumn when the load is low, or during reactions to faults in the system particularly at times of high load when the system is more stressed. The operational parameters (e.g. voltage, active power) could go beyond operational security limits. In extreme cases, it could lead to islanding parts of the system and/or a blackout. System equipment could be damaged as a result of the error.

Crisis Scenario 15– Serial equipment failure

This scenario can materialise at any time, due to a systematic failure in manufacturing. All elements of the same type or series are assumed to be susceptible to the same failure. All suspected elements are assumed unsafe but can't all be immediately replaced or repaired.

Multiple faults, especially occurring in a short period, may lead directly to power supply interruption, as well as cascading events and in extreme cases, to blackouts. Furthermore, equipment may be derated or shut-down as a preventive measure.

Crisis Scenario 16 – Strike, riots, industrial action

This scenario can materialise at any time. The initiating event may involve disputes of some kind that lead to industrial action at scale. It also may include riots, blockades or other massive social unrest (regardless of motivation or inspiration). As a direct consequence, staff in the energy sector (power plants, transmission and distribution) refuse to work, work to rule or are prevented from work. This can result in generation inadequacy, increased likelihood of human error, and longer reaction times in case of faults.

Crisis Scenario 17 – Industrial/nuclear accident

This scenario can occur at any time and is initiated when a serious industrial accident occurs (e.g. an explosion, toxic substance release, etc.) due to any reason (technical failure, earthquake, sabotage, terrorist attack, human error, etc.).

In case of an accident, if power plants are shut down, electricity supply may be reduced for a prolonged time. In a worst-case scenario and due to the small, isolated nature of the Cyprus system, a partial or total blackout is possible, with the possibility of long-lasting lack of adequacy, as important parts of the system are damaged and out of service.

Crisis Scenario 18 – Unusually big RES forecast errors

This scenario may be initiated by remarkably different levels of electricity generation of renewables generation units (wind or solar) due to unusually big forecasting errors, errors in forecast data or fast and unforeseen weather changes. It is most likely to occur in winter when the weather is more variable.

A big shortfall in renewable generation could lead to temporarily insufficient power generation on the system and forced demand curtailment. There could be a limitation of ancillary services. The needed amount of downregulation may not be available which may lead to RES curtailment, or the necessary additional generation may not be available.

Crisis Scenario 19 – Pandemic

The scenario would be initiated at any time by the international spread of a disease. Infections could happen at Control Centres, power stations, power plants and the DSO, which could lead to insufficient staff. Furthermore, containment measures of governments might place restrictions for operation directly or indirectly.

Depending on the spread of the pandemic, the impacts on the power system may vary, but could include limitations in the availability of generation units. It could also lead to an increased risk of human errors. Furthermore, reduced personnel availability may result in increased response times to failures.

Crisis Scenario 20 – Heatwave

This scenario is initiated due to a prolonged heat wave, ie. extremely high temperatures for several days or even weeks and is relevant for the summer.

In general, this scenario assumes stable power system conditions with the following conditions:

- Increased demand for air conditioning due to the heat wave,
- Extremely low generation from wind turbines,
- Some key generators are in emergency maintenance.

These could result in very tight operational security margins and/or create adequacy issues. Furthermore, the weather conditions might trigger equipment failures, particularly on the distribution system.

Crisis Scenario 21 – Earthquake

The scenario would be initiated at any time by the occurrence of a significant magnitude earthquake. The earthquake could damage transmission infrastructure and power plants.

Damage to power infrastructure may result in the unavailability of transmission elements and power plants and possible load shedding to keep system security functioning during peak hours or all the time. Damage to key power stations and/or substations could lead to a black out, persistent adequacy issues, an inability to serve certain areas and/or persistent split of the system into islands.

Crisis Scenario 22 – Forest fire

This scenario is more relevant during the summer months, when temperatures are higher, and precipitation is almost non-existent. It is more likely to be severe during windy days. Load is likely to be high, due to the hot weather.

Forest fires could start and spread because of the wind combined with a dry and hot period. The fires cannot be controlled for days. Uncontrolled wildfires may initiate unavailability or inoperability of some transmission and distribution infrastructure, with one transmission line that crosses the mountain forest being particularly at risk. This may trigger structural degradation or violation of N-1. There may be load reduction and/or load shedding and even a partial blackout, with villages on the Troodos mountain being at most risk.

1.6. Non-relevant regional crisis scenarios

Even though the identification of the national crisis scenarios was based on the regional crisis scenarios, some of the regional crisis scenarios were not considered relevant for the case of Cyprus for certain reasons. Table 7 lists the regional scenarios that were deemed as not relevant for Cyprus, together with a short justification for their rejection.

Table 7: Non-relevant regional crisis scenarios

ENTSO-E Scenario	Description	Reason for rejection
2	Cyberattack – entities not connected to electrical grid	The Cyprus electricity market is still under development. Hence, there are no market entities not connected

		to the grid that could cause an electricity crisis, if compromised.
7	Solar storm	Cyprus does not have long transmission lines and is located in southern Europe, hence it is less vulnerable to solar storm events.
8	Volcanic eruption	Cyprus does not have any volcanoes and is too far from Iceland to be directly affected by volcanic ash.
9	Storm	Cyprus is too far from the Atlantic, and therefore does not experience the type of storms described in this scenario (eg. storm lasting 3 days, with average wind >150km/h and gusts >200km/h).
10	Cold spell	Being a small island at the south-eastern corner of the Mediterranean, Cyprus does not experience temperatures 10°C-20°C below average for 3 weeks, as described in this scenario. Furthermore, electricity generation wouldn't be affected by freezing temperatures, as there is no hydro generation, and cooling water for power stations is obtained from the sea which never freezes in the Mediterranean.
14	Nuclear fuel shortage	Cyprus does not have any nuclear generation.
21	Unwanted power flows	Not applicable to isolated systems.
25	Unforseen interaction of energy market rules	The Cyprus electricity market is still under development. Furthermore, this scenario is unlikely to materialise in a small, isolated system with an ISP and a dominant conventional generator.
29	Dry period	Cyprus does not have any Hydro generation and uses sea water for power station cooling.

ROLES AND RESPONSIBILITIES OF THE COMPETENT AUTHORITY

The Cyprus Energy Regulatory Authority's (CERA) main objective is to design and implement a comprehensive set of regulatory measures and actions that will prepare Cyprus to participate in a smooth, organized and efficient way, in the process of incorporating into the integrated European energy market. At the same time, it must safeguard the necessary security of energy supply in the country, both on a physical and an economic level, and to ensure energy costs accessible to the national economy and the consumer.

CERA has been designated as the competent authority for implementing and carrying out the tasks provided in the Regulation (EU) 2019/941.

According to the Law Regulating the Electricity Market of 2021, L.130(I)/2022, in case of war or other public danger, the Council of Ministers may declare a state of energy crisis, and in such a case, CERA is obliged to follow the procedure provided for in the provisions of paragraph 2 of article 14 of Regulation (EU) 2019/941 regarding the declaration of a state of electricity crisis.

With respect to the Risk Preparedness Plan, CERA is responsible for the establishment of such plans. More precisely, CERA approves certain procedures and measures provided by the TSOC that are part of the Risk Preparedness Plan.

PROCEDURES AND MEASURES IN THE ELECTRICITY CRISIS

1.7. National procedures and measures

With reference to the national crisis scenarios identified, procedures and measures are in place to minimise the likelihood of the crisis scenarios materialising, where possible, and to mitigate the consequences of crisis scenarios in case they materialise. The most important procedures and measures can be summarised under the following categories:

1. Prevention/mitigation of a total or partial system blackout
2. Mitigation of lack of generation adequacy.
3. System preparation for known periods of increased demand, where the system operates close to its stability limits (stress), ie. the hot summer months
4. Arrangements for emergency operation of the National Energy Control Centre (NECC)
5. Physical and Cyber security measures

Table 8 summarises the prevention and mitigation measures that are applicable to each of the identified crisis scenarios. It should be noted that the defined Action Plans provided in the table have a two-fold role to play in tackling all challenges raised from the identified Crisis Scenarios. Firstly, the Action Plans act as a prevention measure, where all critical scenarios are classified and all prevention methods to be followed are portrayed. Secondly, the Action Plans are also considered as a mitigation measure due to the fact that all detailed steps, for addressing the potential occurrence of the classified critical scenarios, are explicitly described.

It should be emphasised that TSOC has long standing and detailed procedures and measures for the risks identified through the process of Regulation (EU) 2019/941. It should also be noted that the TSOC submits annually to CERA for approval certain action plans (Action Plan for System Restoration after a total blackout and Action Plan for electricity crisis during summer period) related and linked to the procedures and measures already mentioned. More details on these are provided in the subsections that follow.

Furthermore, the TSOC's and the Distribution System Operator's (DSO) technical staff at district Areas participate in the Earthquake National Plan "EGKELADOS".

Table 8: Prevention and mitigation measures for each scenario

Crisis Scenario	Name	Prevention	Mitigation
1	Cyberattack – entities connected to electrical grid	• National Cybersecurity Strategy* • Information Security and ICT Systems Resilience*	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Procedure for Informing the Public During an Electricity Crisis*
2	Physical attack – critical assets	• National Energy Control Centre (NECC) Security and Resilience* • Security measures for accessing significant power plants, substations, and TSO premises	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Cyclic Load Shedding Scheme* • Procedure for Informing the Public During an Electricity Crisis* • Network development for redundancy (TYNDP)* • Availability of alternative supply routes via the DSO network at major load centres
3	Physical attack –	• Information Security	• Action Plan for

	control centres	and ICT Systems Resilience* • National Energy Control Centre (NECC) Security and Resilience*	System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • National Energy Control Centre (NECC) Security and Resilience* • Procedure for Informing the Public During an Electricity Crisis* • Protection and control strategies ensure the continued safe operation of the system in case of loss of the SCADA
4	Threat to key employees	• Information Security and ICT Systems Resilience* • National Energy Control Centre (NECC) Security and Resilience*	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • National Energy Control Centre (NECC) Security and Resilience* • Procedure for Informing the Public During an Electricity Crisis* • Network development for redundancy (TYNDP)*
5	Insider attack	• Information Security and ICT Systems Resilience* • National Energy Control Centre (NECC) Security	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding

		and Resilience*	Schemes* • Over-frequency protection scheme* • National Energy Control Centre (NECC) Security and Resilience* • Procedure for Informing the Public During an Electricity Crisis* • Network development for redundancy (TYNDP)*
6	Precipitation and flooding	• Drainage system for substations and power plants (TYNDP)*	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Procedure for Informing the Public During an Electricity Crisis* • Availability of alternative supply routes via the DSO network at major load centres
7	Winter Incident	• Overhead equipment lightning resilience (surge arresters, auto-reclosing relays) (TYNDP)*	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Procedure for Informing the Public During an Electricity Crisis* • Network development for redundancy (TYNDP)*

8	Fossil Fuel Shortage	• Centralised strategic LFO reserves held by COSMOS, with priority access for the Electricity Authority, which are sufficient for operating approximately 1/3 of the installed conventional capacity for 1 month. • Use of two different importing and storage facilities • Two different types of oil (HFO and LFO) used in generation • Ability to import fuel from any player in the international markets, via oil tankers	• Cyclic Load Shedding Scheme* • Procedure for Informing the Public During an Electricity Crisis* • Government support schemes to improve building efficiency and increase RES penetration. Financial support for home insulation and home PV has increased, as a response to increased fuel costs after the Ukraine war.
9	Local technical failure	• Regular maintenance of equipment and upgrades	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Cyclic Load Shedding Scheme* • Procedure for Informing the Public During an Electricity Crisis* • Network development for redundancy (TYNDP)* • Standards for substation design – preventing propagation of a failure

			• Availability of alternative supply routes via the DSO network at major load centres
10	Multiple failures caused by extreme weather	• Action Plan for Electricity Crisis During the Summer Period*	• Action Plan for System Restoration After a Total Blackout* • Action Plan for Electricity Crisis During the Summer Period* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Procedure for Informing the Public During an Electricity Crisis* • Network development for redundancy (TYNDP)* • System design for the most extreme summer temperatures that can happen in Cyprus (TYNDP)*.
11	Loss of ICT systems for real-time operation	• Information Security and ICT Systems Resilience* • National Energy Control Centre (NECC) Security and Resilience*	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Procedure for Informing the Public During an Electricity Crisis* • Protection and control strategies ensure the continued safe operation of the

			system in case of failure of communication systems
12	Simultaneous multiple failures	• Action Plan for Electricity Crisis During the Summer Period*	• Action Plan for System Restoration After a Total Blackout* • Action Plan for Electricity Crisis During the Summer Period* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Procedure for Informing the Public During an Electricity Crisis* • Network development for redundancy (TYNDP)*
13	Power system control mechanism complexity	• Main and back-up protection functions on the system.	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Procedure for Informing the Public During an Electricity Crisis*
14	Human error	• Information Security and ICT Systems Resilience* • National Energy Control Centre (NECC) Security and Resilience* • Reduce by design the likelihood of occurrence of human error (eg. Interlocks, control	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Procedure for Informing the Public During an Electricity

		functions design) • Training • Certification process for staff who are allowed to work on and/or perform operations on the transmission and distribution systems	Crisis* • Network development for redundancy (TYNDP)*
15	Serial equipment failure	• Advanced warning when systematic equipment failures are discovered internationally, via the Asset Management Forum that EAC participates in.	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Procedure for Informing the Public During an Electricity Crisis* • Network development for redundancy (TYNDP)* • More frequent inspection and maintenance regime, including additional maintenance steps where required, when systematic equipment failures are discovered. • Additional safety measures in accessing and/or operating affected equipment, where required.
16	Strike, riots, industrial action	• Industrial Relations Code of the Ministry of Labour, adopted by the Electricity Authority and its Trade Unions	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes*

			• Over-frequency protection scheme* • Cyclic Load Shedding Scheme* • Information Security and ICT Systems Resilience* • National Energy Control Centre (NECC) Security and Resilience* • Procedure for Informing the Public During an Electricity Crisis* • Network development for redundancy (TYNDP)* • Reduce by design the likelihood of occurrence of human error (eg. Interlocks, control functions design)
17	Industrial/nuclear accident	• Network design (TYNDP) and appropriate equipment installation	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Cyclic Load Shedding Scheme* • Procedure for Informing the Public During an Electricity Crisis* • Network development for redundancy (TYNDP)*
18	Unusually big RES forecast errors	• Grid code obligations on RES producers for the quality of their forecasts. • TSO co-operation	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding

		with academic institutions for improving PV forecasts.	Schemes* • Over-frequency protection scheme* • Procedure for Informing the Public During an Electricity Crisis* • Fast-start OCGTs
19	Pandemic	• Business Continuity based on the Ministers' Decree per case	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Cyclic Load Shedding Scheme* • Information Security and ICT Systems Resilience* • National Energy Control Centre (NECC) Security and Resilience* • Business Continuity During a Pandemic* • Procedure for Informing the Public During an Electricity Crisis* • Network development for redundancy (TYNDP)* • Reduce by design the likelihood of occurrence of human error (eg. Interlocks, control functions design)
20	Heatwave	• System design for the most extreme summer temperatures that can happen in Cyprus (TYNDP).	• Action Plan for System Restoration After a Total Blackout* • Action Plan for Electricity Crisis During the Summer Period*

			• Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Cyclic Load Shedding Scheme* • Procedure for Informing the Public During an Electricity Crisis* • System design for the most extreme summer temperatures that can happen in Cyprus (TYNDP).
21	Earthquake	• Earthquake National Plan "EGKELADOS"	• Action Plan for System Restoration After a Total Blackout* • Under-frequency Load Shedding Schemes* • Over-frequency protection scheme* • Cyclic Load Shedding Scheme* • Procedure for Informing the Public During an Electricity Crisis* • Network development for redundancy (TYNDP)* • Infrastructure designed to local earthquake resistance codes (TYNDP)* • Earthquake National Plan "EGKELADOS"
22	Forest fire	• Action Plan for Electricity Crisis During the Summer Period* • Pilot project between EAC and	• Action Plan for System Restoration After a Total Blackout* • Action Plan for Electricity Crisis

	UCY (KIOS CoE) to check the integrity of transmission lines through forests and the proximity of vegetation to the lines, via drones	During the Summer Period* • Over-frequency protection scheme* • Procedure for Informing the Public During an Electricity Crisis* • Network development for redundancy (TYNDP)* • Planned upgrades will make the most vulnerable line more resilient (TYNDP)*
***More details are provided in the following sections.**		

1.8. Detailed Descriptions of Key National Procedures and Measures

1.8.1. Action Plan for System Restoration After a Total Blackout

Topics covered:

- Prevention/mitigation of a total or partial system blackout

Scenarios applied:

- Due to the small, isolated nature of the Cyprus power system, this is applicable to all scenarios except Scenario 8 - Fossil fuel shortage.

TSOC, in fulfilling its duty to ensure a safe and reliable operation of the Electrical System, has prepared the "Action Plan for System Restoration after a Total Blackout" which is reviewed and updated annually. This Action Plan, which comprises of the General Plan and a number of Sub-Plans, defines the proposed processes/actions for various system restoration scenarios after a Total Blackout. It should be noted that the same procedures can also be applied in the case of a Partial Blackout.

All parties involved in the process of restoring the system after a Blackout, that are: the NECC, the Power Stations, the Transmission and Distribution System

District and Central Offices, have prepared Sub-Plans regarding the initial processes/actions to be followed in case of a Blackout, in preparation for the execution of the General Action Plan that is activated and coordinated by the NECC. These include, for example, contact details and responsibilities of key personnel, alert and communication mechanisms, and actions of the relevant party. It should be noted that the plan also details actions to be followed in case some of the above steps fail or in case the SCADA System is unavailable (several restoration scenarios are described).

The Action Plan is activated when the NECC establishes that the system is in a total black out. The NECC informs the TSOC managers and operation department, as well as designated co-ordinators at each District and each Power Station, who in turn ensure that the personnel designated in their sub-plans will be the soonest at their designated posts (eg. key substations and power stations with black start capability), awaiting further instructions from the NECC. The NECC co-ordinates the system restoration process.

The following figure 1 illustrates the actions followed by the TSOC in case of a Total Blackout Scenario.

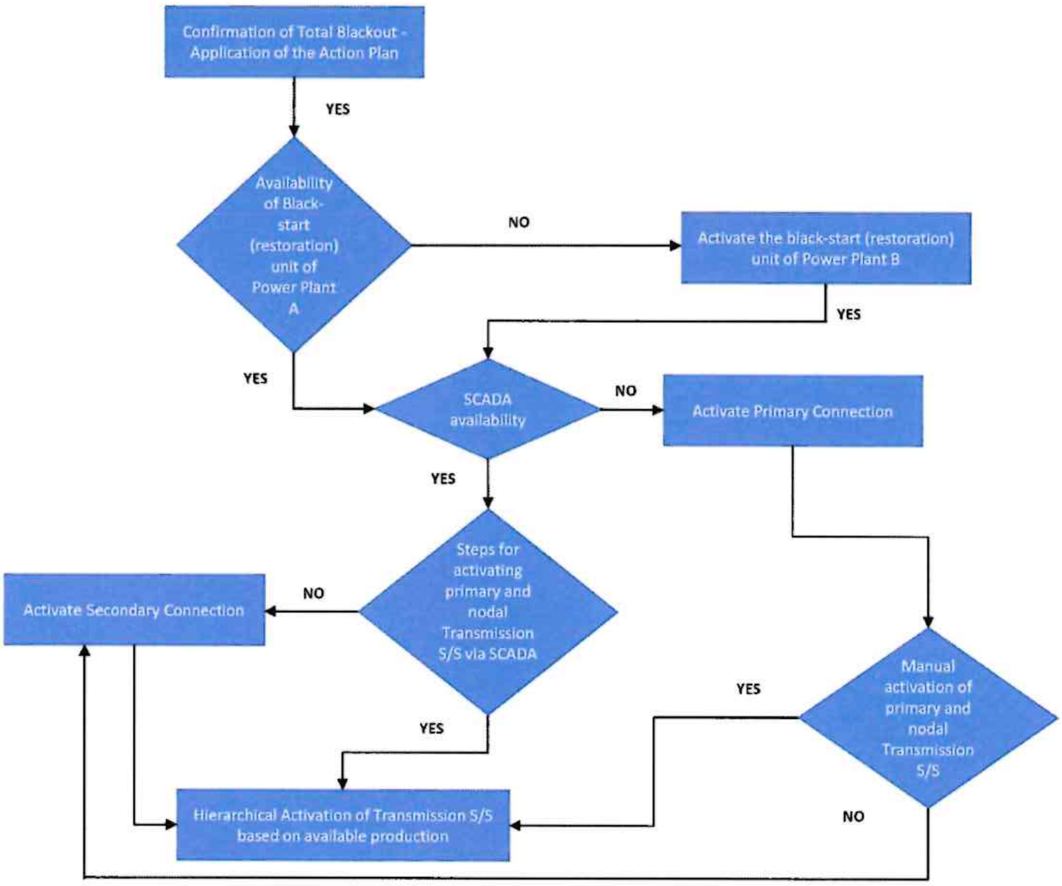


Figure 1: Actions followed by the TSOC in case of Total Blackout Scenario.

1.8.2. Action Plan for Electricity Crisis During the Summer Period

Topics covered: • System preparation for known periods of stress, i.e. the hot summer months • Mitigation of lack of generation adequacy Scenarios applied:

- Scenario 10 - Multiple failures caused by extreme weather
- Scenario 12 - Simultaneous multiple failures
- Scenario 20 - Heatwave
- Scenario 22 - Forest fire

For the case of Cyprus's power system, the summer period is the time of year during which the electricity system faces the most stress, due to the high electricity demand resulting from the high summer temperatures. Therefore, TSOC has put in place an Action Plan to cope with an Electricity Crisis during this period, which is reviewed and updated at the beginning of every summer.

The Action Plan:

- Examines system adequacy, in light of forecast demand and generation unit availability for the summer period.
- Examines transmission system resilience, through the application of the N-1 security criterion.
- Defines preventive actions to ensure that the system is in the best possible place to cope with stresses. These include ensuring that there are no planned generation or transmission system maintenance activities during the summer period, that transmission line bushings have been washed before the start of the period, that there is availability of spares to deal with faults, and that backup power supplies are operational.
- Defines roles and responsibilities and information flows in case of an emergency. More specifically, co-ordinators are appointed for the purposes of this Action Plan by all relevant parties, i.e. the Transmission System Operator, Transmission System Owner, Distribution System Operator, Distribution System Owner and Generation Owners.
- Defines the process for informing the public.

The Action Plan contains actions that take place before the start of the summer period to prevent an electricity crisis without requiring the plan to be activated, as well as measures and procedures to cope with an electricity crisis if it materialises. The Action Plan is activated when the Transmission System Operator deems that an electricity crisis may be imminent, due to high demand and/or high unavailability of generators. The TSO co-ordinates the actions required, through communication with the designated personnel of the power stations, the transmission system owner and the distribution system operator. The latter must be ready for a possible activation of the Action Plan throughout the summer period.

System stability in case of faults that result in loss of generation is ensured through the automatic Under Frequency Load Shedding Scheme (UFLS). Furthermore, a cyclic load shedding scheme is in place for cases of lack of generation adequacy.

It should be noted that the actions and procedures to be followed in case of an electricity crisis, as detailed in the Action Plan, can be applied to an electricity crisis happening at any time of the year.

During the Summer period and whenever this is necessary, the DSO's District Offices issue rosters for standby Technical Personnel to cope with emergencies, such as multiple distribution network faults. Additionally, DSO activates a plan to improve the 24h local Call Centres response and handling of massive incoming calls.

1.8.3. Under Frequency Load Shedding Schemes

Topics covered: • Prevention/mitigation of a total or partial system blackout Scenarios applied: • All scenarios except Scenario 8 – Fossil fuel shortage and Scenario 22 –

Forest fire

An automatic Under Frequency Load Shedding scheme (UFLS) is in place. The scheme consists of 13 stages which are progressively triggered as the frequency gets lower, and it is designed to disconnect up to approximately 68% of the system load. The first stage is triggered at 49.0Hz with a delay of 200ms, while the last stage is triggered at 47.5Hz with a delay of 350ms. To ensure a quick arrest of the frequency drop in case of a severe imbalance, which is a possibility due to the small, isolated nature of the system, ROCOF relays are additionally installed on some feeders predominantly in the first 4 stages of the UFLS, which are triggered when the rate of change of frequency exceeds 1 Hz/s for 300ms and disconnect approximately 6% of the system load.

The stages have been prepared in co-operation with the DSO, ensuring uninterrupted power supply to critical services such as hospitals and airports, and important areas of economic activities. Furthermore, certain vulnerable customers whose life depends on electricity supply, are entitled to receive special protection against disconnection. The scheme is regularly reviewed, for example taking into account the increasing penetration of PV generation at certain substations.

In addition to the above scheme, a Delayed Under Frequency Load Shedding scheme is triggered if the frequency remains below 49,5Hz for more than 20s, with the aim to restore frequency to the normal operating limit. This scheme consists of a number of stages, which disconnect additional loads amounting upto approximately 15% of the system load from the Stages of the automatic UFLS.

Where manual load shedding is required, the system provides the operators at the NECC the ability to easily disconnect predefined groups of loads. The first to be manually disconnected are water pumps and tele-controlled heating/air-conditioning, which are loads of low importance. Further disconnection groups have been created with loads taken from the Stages of the automatic UFLS.

1.8.4. Over Frequency Protection Scheme

Topics covered: • Prevention/mitigation of a total or partial system blackout Scenarios applied: • All scenarios except Scenario 8 – Fossil fuel shortage

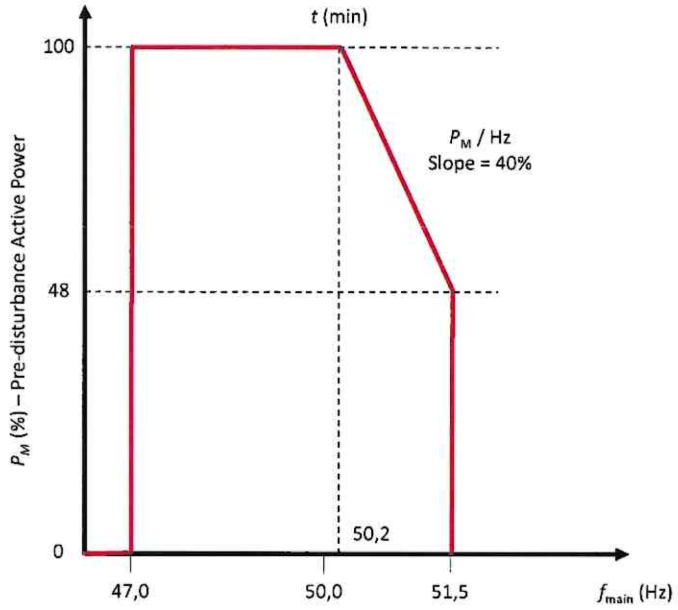
Automatic RES curtailment schemes are in place, which are activated in case of over-frequency.

Large wind parks, which have a connection agreement with the TSO, are obliged to curtail their output, with a delay of 400ms, as follows:

- 65% of their pre-disturbance output when the frequency reaches 50,25Hz
- 30% of their pre-disturbance output when the frequency reaches 50,50Hz
- 0% of their pre-disturbance output when the frequency reaches 50,70Hz

In order to ensure that RES active power recovery, when frequency recovers to within normal limits, does not introduce an over-frequency disturbance, each power park is given an individual active power recovery plan that it must adhere to, with a specified time delay and a specified rate of active power increase.

Small RES, which have a connection agreement with the DSO, are obliged to continuously follow the below active power curtailment curve during over-frequency events.



1.8.5. Cyclic Load Shedding Scheme

Topics covered:

- Mitigation of lack of generation adequacy

Scenarios applied:

- Scenario 2 – Physical attack – critical assets
- Scenario 8 – Fossil fuel shortage
- Scenario 9 – Local technical failure
- Scenario 16 – Strike, riots, industrial action
- Scenario 17 – Industrial/nuclear accident
- Scenario 19 – Pandemic
- Scenario 20 – Heatwave

- Scenario 21 – Earthquake

A cyclic load shedding scheme is in place and ready to be deployed in cases of lack of generation adequacy. The scheme facilitates rolling power cuts to 22 groups of loads across the island. The groups have been prepared in co-operation with the DSO, ensuring uninterrupted power supply to critical services, such as hospitals and airports, and important areas of economic activities such as industrial zones/areas and tourist areas. In addition, certain vulnerable customers whose life depends on electricity supply, are entitled to receive special protection against disconnection. The scheme is regularly revised, taking into account for example the increasing penetration of PV generation at certain substations.

The scheme is activated for the day ahead when the TSO expects a lack of generation adequacy. TSOC uses their in-house software to estimate the load shedding cycle for each Group for the day ahead and prepare a cyclic load shedding schedule for the NECC to follow, based on forecast demand and generation unit availability. Subsequently, the public is informed, via press releases, of the time and duration of the power cuts to their area. In periods of prolonged lack of adequacy, the press releases may cover the rolling power cut timetable for longer periods e.g. a week.

1.8.6. National Cybersecurity Strategy

Topics covered: • Physical and Cyber security measures Scenarios applied: • Scenario 1 - Cyberattack – entities connected to electrical grid

The main objective of the Cybersecurity Strategy of the Republic of Cyprus is the protection of critical information infrastructure of the Republic and setting appropriate security standards for the communication technologies used for the common benefit and the economy of Cyprus. A holistic approach has been adopted to deliver a multilevel security strategy, considering the rapid evolution of cyberspace threats which are imposed on critical information systems.

National legislation exists in the Republic of Cyprus, sufficiently covering all cybersecurity matters. Nonetheless, updates and modifications to the existing Law are constantly required to comply with new European directives and to cover specific provisions of the cybersecurity strategy of the Republic of Cyprus. Primary and secondary legislation has been enforced regarding cybersecurity stipulated under Law N.89(I)/2020, decisions KDP 389/2020 [4]and KDP 41/2022[5]. This legislative framework ensures that all requirements presented through EC Directives, the EU Cybersecurity package, ENISA regulations, GDPR and more, are clearly integrated in Cyprus Law. The objective of these commitments is the creation of a highly secure cyberspace in all critical sectors, therefore setting the foundations for further exploitation of digital technologies in Cyprus.

The Digital Security Authority (DSA) is the competent authority assigned with the task of creating a structural framework, under which all cybersecurity matters are addressed. Achieving this task requires actions in risk management, strategy

[4] Security Measures of Operators of Basic Services and Operators of Critical Information Infrastructure Decision of 2020 (K.D.P. 389/2020)
[5] The Security of Networks and Information Systems (Security Measures of Network and/or Electronic Communications Service Providers) Decision of 2022 (C.D.P. 41/2022)

assessment, measure development, danger assessment and incident/ crisis management. A national cybersecurity framework is developed outlining the methodology which must be used by competent authorities and critical information carriers, in order to mitigate potential cybersecurity threats.

A Contingency Plan for critical informatics infrastructure has been developed for the guidance and development of detailed procedures to be followed when a large-scale crisis impacts the operation of critical informatics infrastructure. The Contingency Plan is to be reviewed and revised regularly based on the findings of national danger assessment reports and external factors which could affect the operation of the critical informatics infrastructure. More specifically based on the National Contingency Plan, the following actions are considered for handling the event of a crisis:

- Categorization and hierarchical arrangement of crucial infrastructure, based on their contribution on supporting vital communication and informatics services, as well as based on results from the findings of the national danger assessment reports.
- The development of "early warning" systems and procedures for infrastructure monitoring using the expertise of the national CSIRT.
- The development or improvement of emergency communication networks, unrelated to main networks, and if possible, using separate communication mediums.
- The complete development of communication and management procedures in the event of a crisis between administrators of critical informatics infrastructure, so that optimal coordination and cooperation is achieved.
- Conduct periodic national workshops tackling realistic crisis scenarios for the test and improvement of the above procedures
- Management of resources on a hardware and infrastructure level, where deemed necessary, between involved services and organisations, with the

aim of forming redundancy links fortifying the infrastructure in the event of a crisis.

According to DSA's decision KDP 389/2020 and its amendments[6], each carrier of critical informatics infrastructure is obliged to abide by regulations and procedures as stipulated by Cyprus Law. These minimum requirements include producing annual risk assessment reports for their networks and critical infrastructure and submitting them to the DSA along with a coherent business continuity plan based on the findings of each report which includes detailed measures and provisions taken for security incidents and crisis scenarios. Additionally, measures should be taken in accordance with the security management framework, in order to manage potential dangers, prevent and minimise the effect of incidents as well as ensure safety and service continuity after a potential attack. On a physical level, the carrier must monitor the performance of its networks and critical infrastructure on a real-time basis to ensure no faults are occurring or imminent. Additionally, personnel should be available on standby to provide immediate response to any incident outside of working hours. The physical condition of the equipment should be monitored closely with onsite security as well as physical backups for additional redundancy. In addition to national legislations, carriers must abide by all regional and communal regulations regarding provisions and standards of cybersecurity and critical infrastructure safety. A Chief systems and network security officer must be appointed by each carrier to ensure compliance with the above cybersecurity provisions and maintain active communication with the DSA.

In respect to the transmission system, the distribution system and the critical infrastructures (where applicable), the TSO, the DSO and the owner of the critical infrastructures should follow the guidance of the National Digital Security Authority.

[6] On the Amendment of the Security of Networks and Information Systems (Security Measures of Operators of Basic Services and Operators of Critical Information Infrastructure) Decision of 2020, Decision of 2022 (K.D.P. 40/2022)

1.8.7. Information Security and ICT Systems Resilience

Topics covered:

- Physical and Cyber security measures

Scenarios applied:

- Scenario 1 - Cyberattack – entities connected to electrical grid
- Scenario 3 – Physical attack – control centres
- Scenario 4 – Threat to key employees
- Scenario 5 - Insider attack
- Scenario 11 - Loss of ICT systems for real-time operation
- Scenario 14 - Human error
- Scenario 16 - Strike, riots, industrial action
- Scenario 19 - Pandemic

TSOC has in place physical (e.g. access control, CCTV, alarm system, fire detection system) and logical security measures (e.g. firewall, Intrusion Detection and Prevention System, antivirus, web protection, email protection, network segmentation, DMZ zone, user access on least privilege principle) in order to secure the network and information of the organisation.

The system and information resilience is achieved through backups, Uninterruptible Power Supply (UPS), generator, redundancy systems and disaster recovery sites. Furthermore, the electricity system can continue operation in case of ICT systems failure.

TSOC SCADA Infrastructure is interconnected by a proprietary Network. Further to the intelligent secured perimeter of the Network, a strong segmentation is used between subsystems and also deep analysis and detection of SCADA communication protocols is performed.

Resilient communications between the NECC and critical locations across the system (eg. substations, power stations) are ensured via a radio frequency communication system owned and maintained by the EAC. This ensures that communication between critical personnel is possible during times of crisis (eg. total black out), even when the public telecommunications systems fail.

Cyber-incidents are properly identified as a risk at the Cyprus' national electricity crisis scenarios analysis, and certain measures are taken to address them. TSOC applies the most recent security standards for new installations. In order to avoid malicious attacks, any device or applications connected to the SCADA system, is governed by strong cybersecurity strategies in procedures and policies. Moreover, the Market Management System (MMS) is being developed in compliance with the NIS Directive.

Furthermore, taking into account the NIS Directive (EU 2016/1148) concerning general rules on security of network and information systems, both the TSOC and DSO are following the guidelines as imposed by the Cybersecurity Strategy of the Republic of Cyprus.

As part of its cyber-security strategy, TSOC performed, in the 4th quarter of 2021, a Risk Assessment for both IT and SCADA Infrastructure with the objective to protect (Identify and Remediate of vulnerabilities) all critical infrastructure and data from damage, attack, or unauthorised access. Moreover, TSOC performed a penetration test (Internal & External) to check for exploitable vulnerabilities and identify any cyber security issues or weaknesses in TSOC systems, networks or web applications.

Based on the findings of the Penetration test, TSOC is in the process of implementing fixes and mitigation measures (e.g. further network segmentation, installation of new frond-end routers, Microsoft 365 security hardening, Multi-Factor Authentication, etc) for any vulnerabilities or weaknesses found. After completing this process, the penetration testing will be repeated in order to verify that the findings are mitigated.

TSOC also created a Business Continuity Plan and an Information Security Policy and is preparing more policies regarding information security.

1.8.8. National Energy Control Centre (NECC) Security and Resilience

Topics covered:

- Prevention/mitigation of a total or partial system blackout
- Arrangements for emergency operation of the National Energy Control Centre
- Physical and Cyber security measures

Scenarios applied:

- Scenario 2 – Physical attack – critical assets
- Scenario 3 – Physical attack – control centres
- Scenario 4 - Threat to key employees
- Scenario 5 – Insider attack
- Scenario 11 – Loss of ICT systems for real-time operation
- Scenario 14 – Human error
- Scenario 16 – Strike, riots, industrial action
- Scenario 19 – Pandemic

A number of measures are in place to secure the operation of the NECC, as follows:

There is an emergency control centre which can be used in a crisis situation. A procedure is in place for the switching of operations from the main to the emergency control centre when required. Furthermore, in 2022, TSOC conducted a drill of manning and operating the emergency control centre.

A backup power supply is available for the NECC and SCADA in case of a blackout.

A plan is in place for utilising TSOC day personnel who have received appropriate training to staff the NECC in case of an emergency.

Access to the NECC is physically restricted to authorised personnel.

The NECC is guarded by a 24-hour security service.

1.8.9. Business Continuity During a Pandemic

Topics covered: • Arrangements for emergency operation of the National Energy Control Centre Scenarios applied: • Scenario 19 - Pandemic

During a pandemic situation, such as COVID-19, TSOC and DSO implement all the directives and protocols issued by the competent authority, which is the Ministry of Health. Additionally, TSOC's and DSO's Health and Safety teams continuously monitor the evolving situation and government advice, and they can make recommendations for additional preventive measures over and above those mandated by the Ministry.

In addition, DSO implements extended measures to minimise the virus transmission within the organisation by separating the office staff into two groups, those working in house and those working remotely. Apart of this, to limit the virus spread into small number of cases, DSO divides the technical personnel into groups and distributes them at geographically different work base locations.

Particular attention is paid to the NECC, where shift patterns are adjusted to minimise contact of personnel from different shifts. Furthermore, TSOC ensures that a number of day personnel are trained to staff the NECC shifts in case of emergency.

1.8.10. Procedure for Informing the Public During an Electricity Crisis

Topics covered: • Prevention/mitigation of a total or partial system blackout • Mitigation of lack of generation adequacy Scenarios applied: • All scenarios

With regard to transmission system or generation faults that result in a disruption of electricity supply to a significant number of consumers that is expected to exceed 45 minutes, the NECC follows a standardised procedure to issue a press statement based on a predefined template. The information on the template includes:

- the date and time of the incident,
- the cause of the incident and a description of its development into a crisis situation,
- affected area,
- limitation in electricity consumption and generation,

Regarding distribution system faults, the relevant DSO procedures are followed.

Where generation inadequacy is anticipated necessitating the use of cyclic load shedding, the public is informed in advance, via press releases, of the time and duration of expected power cuts to their area.

1.9. State of Preparedness for an Electricity Crisis

If there is a specific, serious and reliable information from the seasonal adequacy assessment or other competent source that an electricity crisis may occur, CERA takes appropriate measures to avoid it and following consultations with involved parties (where appropriate), proceeds with certain preventive and preparatory measures such as:

- Decision to ensure that the conventional generation units which are in working condition and are connected to the system will be technically available for the 'crisis' period and that they will be available to the TSOC for operation whenever required for ensuring electricity demand for and the margin of installed capacity reserve for the electricity system of Cyprus.
- Decision to use temporary conventional generation units that will be technically available for the 'crisis' period and will be available to the TSOC for operation whenever required for ensuring electricity demand.
- Decision to inform consumers about the possible electricity crisis and the measures taken by CERA to deal with it effectively. Decision for request for assistance from other Member States (where possible).

In addition, CERA shall provide an early warning without delay to the relevant national authorities, the European Commission, the competent authorities of the Member State located in the same region and, where they are not located in the same region, the competent authorities of the directly connected Member States. CERA shall also provide information on the causes of a possible electricity crisis and the possible need for assistance from other Member States.

1.10. Market operation in case of crisis

The Cypriot TSO / MO will safeguard the continuity of energy transactions during normal circumstances as well as during crisis situations that can be handled using the available market activities and processes.

Even though the electricity market of Cyprus in not fully operational, the market rules enable demand-side measures and storage assets than can ensure energy security and improve system resiliency both in long term as well as during electricity crisis periods. During such events, market measures are implemented that aim to alter consumption through Demand Response mechanisms that enable the participation of dispatchable load portfolios in the Balancing markets.

The Market Rules provide for their temporary suspension, when the TSO declares the presence of a state of emergency as a last resort measure. The objective of the temporary suspension is to evade the prolongation of market activities that will either negatively affect the safety margins of the system during an emergency or will distort the restoration procedure. During an Emergency State and subsequently the suspension of the Electricity Market, the Integrated Scheduling Process (ISP) is not performed, and all market participants are obliged to follow the guidelines of the TSO, to guarantee that the safety of their personnel and equipment is not jeopardized. A state of emergency may be declared, in line with the Transmission and Distribution Rules. The Transmission and Distribution Rules contain provisions for the following procedures, which can be applied in emergencies:

- Cyclic load shedding
- Automatic Load Shedding
- System recovery after a partial or total black-out

For the application of the abovementioned measures, the percentage of load shedding, curtailment levels of RES production as well as the proportion and geographical distribution of non-available transmission system components are considered. These parameters are used to define the percentage of produced energy which is feasible to be transferred from one TSO area to another as well as the incapacity of market participants to offer balancing services and inability to suppliers to meet the requirements of their demand portfolios.

1.11. Future development that contribute towards addressing electricity crisis scenarios

1.11.1. TSOC's Ten Year Network Development Plan

Topics covered:

- Prevention/mitigation of a total or partial system blackout
- System preparation for known periods of increased demand, where the system operates close to its stability limits (stress), ie. the hot summer months

Scenarios applied:

- Scenario 2 – Physical attack – critical assets
- Scenario 4 - Threat to key employees
- Scenario 5 – Insider attack
- Scenario 6 – Precipitation and flooding
- Scenario 7 – Winter incident
- Scenario 9 – Local technical failure
- Scenario 10 – Multiple failures caused by extreme weather
- Scenario 12 – Simultaneous multiple failures
- Scenario 14 – Human error
- Scenario 15 – Serial equipment failure

- Scenario 16 – Strike, riots, industrial action
- Scenario 17 – Industrial/nuclear accident
- Scenario 19 – Pandemic
- Scenario 20 – Heatwave
- Scenario 21 – Earthquake
- Scenario 22 – Forest fire

TSOC develops the transmission system according to its Ten-Year Network Development Plan, which is revised annually. Because of the frequency and severity of heatwaves in Cyprus, TSOC takes into account extreme temperature conditions in the scenarios that are simulated for producing the TYNPD. Transmission system capacity is added, where required, to ensure that all load can be served under even the most extreme heat waves, while maintaining the N-1 security criterion.

As part of the TYNDP, old infrastructure is upgraded/replaced, and additional redundancy is added where criticalities are identified. For example:

- A new substation will be built in the main power generation and industrial area of the island, which will provide additional routes for exporting power from the area. This will reduce the likelihood of a black-out and/or generation inadequacy in case of a crisis scenario materialising in the area.
- The old transmission line through the mountains will be replaced. This will make it more resilient to weather conditions and fires.

Infrastructure is designed to appropriate standards, including the local earthquake resistance code, and including provisions for adequate drainage of substations. Furthermore, EAC's participation in the Asset Management Forum facilitates an early reaction to systematic equipment flaws.

1.11.2. Interconnections

The construction of interconnections will significantly improve the resilience of the electricity system of Cyprus. The possibility of cross-border electricity flows will be a significant mitigation for scenarios where a possible outcome is generation inadequacy. Such scenarios include those with the possibility of a long-lasting lack of adequacy due to damage to a major power station, such as a physical attack to critical assets or an industrial accident or an earthquake, as well as those with the possibility of a short-term lack of adequacy, such as a heatwave. Issues with RES forecast errors will also be effectively tackled, as cross-border imports/exports can be used to balance any shortfall/excess. Furthermore, the introduction of an additional source of ancillary services to the system is expected to reduce the likelihood of a crisis scenario leading to a severe outcome such as a black-out.

EuroAsia Interconnector, which has PCI status, will interconnect the transmission system of Cyprus with those of Israel and Greece. The bipolar HVDC link will have a nominal capacity of 1000 MW (2x500 MW). The project has received a €657 million grant approval from the CEF and a €100 million grant as part of the Recovery and Resilience Plan for Cyprus. The possibility of interconnecting Cyprus with Egypt, via the EuroAfrica Interconnector, is also being examined. The latter is also envisioned as a bipolar HVDC link with a nominal capacity equal to 1000 MW (2x500 MW).

1.12. Regional and bilateral procedures and measures

Cyprus is an isolated island; therefore, it is excluded from Articles 6, 12 and 15(2) to 15(9) of Regulation 2019/941 and no regional or bilateral procedures and measures are implemented.

CRISIS COORDINATOR

According to the Law Regulating the Electricity Market of 2021, L.130(I)/2022, in case of war or other public danger, the Council of Ministers may declare a state of energy crisis, and in such a case, CERA is obliged to follow the procedure provided for in the provisions of paragraph 2 of article 14 of Regulation (EU) 2019/941 regarding the declaration of a state of electricity crisis.

With respect to the competences provided to CERA and TSOC within the Law Regulating the Electricity Market of 2021, L.130(I)/2021 and for the purposes of implementing the provisions of Regulation (EU) 2019/941 the Director of the TSOC or his legal representative shall be responsible for the overall oversight and coordination of any crisis in the electricity sector related to the Regulation (EU) 2019/941 as addressed in the Risk Preparedness Plan. The Crisis Coordinator should keep informed the Cyprus Energy Regulatory Authority on his action.

The contact details of the Director of the TSOC are the following:

Mr. Stavros Stavrinos
Director
Cyprus' Transmission System Operator
68 Evagelistrias
CY-2057, Strovolos
tel: +357 2227 7000
fax: +357 22 611 666
sstavrinos@dsm.org.cy
mail@dsm.org.cy
www.dsm.org.cy

STAKEHOLDER CONSULTATIONS

As per article 10(1) of the Regulation 2019/941, the mechanism used for the consultations carried out was contacting directly with relevant bodies such as:

- relevant electricity undertakings, including relevant producers or their trade bodies,
- relevant organisations representing the interests of non-industrial electricity customers,
- relevant organisations representing the interests of industrial electricity customers,
- the TSOC, and
- the DSO.

Apart from those entities, CERA decided to consult with the National Digital Security Authority concerning cyber security issues.

Comments were received by the DSO, the EAC-Supply, the Cyprus' Chamber of Commerce and Industry and the National Digital Security Authority. There comments were taken into account and a revised version of the draft plan was prepared.

On 14 June 2022, the COMMISSION OPINION under Regulation (EU) No 2019/941, on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, on the Risk-preparedness Plan submitted by the Competent Authority of Cyprus to the European Commission was communicated to the relevant authorities of Cyprus.

According to the Regulation (EU) 2019/941, within three months of receipt of the Commission's opinion, the competent authority concerned shall take full account of the Commission's recommendation and shall either notify the amended risk-preparedness plan to the Commission or notify the Commission of the reasons why it objects to the recommendation.

CERA, considering the above, consulted with the TSOC and DSO and revised the risk-preparedness plan accordingly.

EMERGENCY TESTS

TSOC conducts, every six months, tests for System Restoration after a Total Blackout, in line with the relevant plan. More specifically, proof tests are performed of the ability of black start generators to be started without the presence of grid power and of the communications between the NECC, the power station control centres and the key transmission system substations.

In addition, the TSOC, the DSO and the critical infrastructures (where applicable) following the guidance of the National Digital Security Authority should examine the development of tests concerning major cyber security incidents and / or crises, which could affect the generation, transmission and distribution of electricity.

LIST OF ACRONYMS AND ABBREVIATIONS

CEF	Connecting Europe Facility
CERA	Cyprus Energy Regulatory Authority
COSMOS	Cyprus Organisation For Storage and Management of Oil Stocks
DSA	Digital Security Authority
DSO	Distribution System Operator
EAC	Electricity Authority of Cyprus
ECG	Electricity Coordination Group
EMS	Energy Management System
ENTSO-E	European Network of Transmission System Operators for Electricity
GDPR	General Data Protection Regulation
GIS	Gas-Insulated Switchgear
ICT	Information and Communications Technology
IT	Information Technology
MMS	Market Management System
MO	Market Operator
NECC	National Energy Control Centre
ODS	Owner of the Distribution System
PCI	Project of Common Interest
RES	Renewable Energy Sources

RPR	Risk Preparedness Regulation (EU) 2019/941
SCADA	Supervisory Control and Data Acquisition
TSO	Transmission System Operator
TSOC	Transmission System Operator – Cyprus
TYNDP	Ten Year Network Development Plan