European Distribution System Operators for Smart Grids

Response to the European Commission's public consultation on risk preparedness in the area of security of electricity supply

October 2015

Executive summary

The European Distribution System Operators for Smart Grids (EDSO) welcomes the European Commission's (EC) public consultation on security of electricity supply.

Security of supply is a pillar of the European energy policy and since they exist, distribution system operators (DSOs) have been entrusted to preserve it. This task is achieved through constant monitoring of the networks, coordinated actions with transmission system operators (TSOs), and in last-resort, load-shedding (i.e., temporary disconnection of grid users).

This last resort action is rarely taken, but with a large number of small generation units connected to distribution networks, growing interest for demand-side response, heat pumps, and electric vehicles, the variability of power flows is increasing and requires additional coordination between all players in the electricity value chain to maintain security of supply.

EDSO has formulated four key recommendations which are further elaborated in this document.

EDSO recommendations to the European Commission:

- Closely involve DSOs in the definition of risk preparedness plans.
- Define or select a common methodology for risk assessments across Europe to foster a shared understanding of risks between Member States.
- If the Electricity Coordination Group is given any additional responsibilities related to security of supply, invite DSOs to join due to their key role in emergency situation.
- Avoid creating an additional authority for monitoring security of supply. However, designating at national level an existing organisation (e.g., ministry, regulator) as responsible for coordinating security of supply issues could be useful.

Current legal framework relating to security of electricity supply

1. Whilst Directive 89/2005 imposes a general obligation on Member States to ensure a high level of security of supply, the Directive does not specify what measures Member States should take to prevent risks. Would there be an added value in requiring Member States to draw up a plan identifying relevant risks and preventive measures to respond to such risks (risk preparedness plans)?

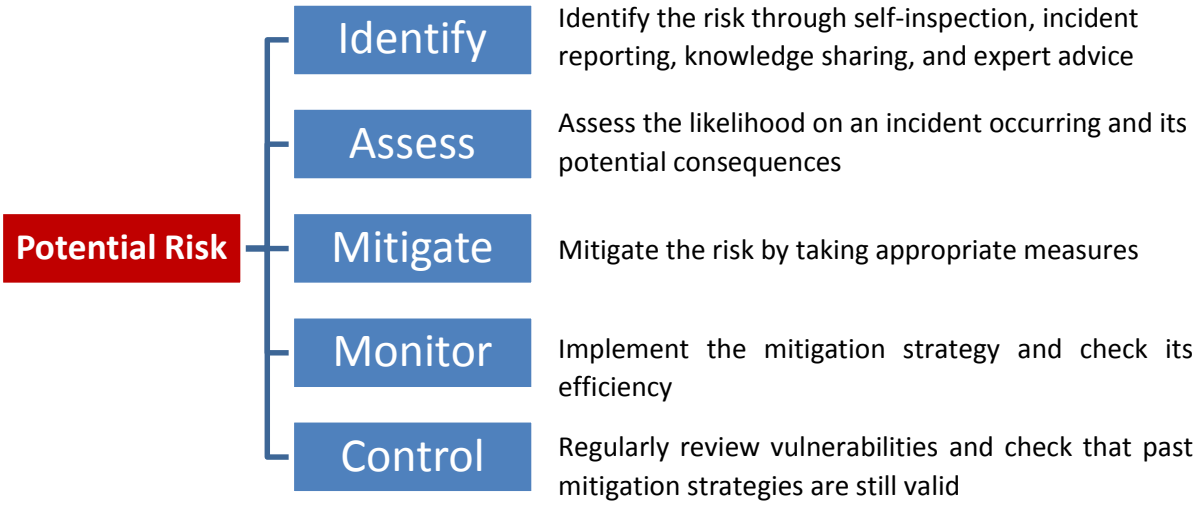
Today, transmission and distribution system operators are in charge of security of supply and prepare on a regular basis their own emergency and restoration plan. These procedures are currently being harmonised by ENTSO-E and all relevant stakeholders who contributed to the drafting of the Emergency and Restoration network code.

Nonetheless, this future piece of legislation will only cover electricity networks. The preventive actions to be taken by other sectors in case of outage are not defined in this document. National risk preparedness plans appear necessary to mitigate the impact of any interruption of supply and make society more resilient to any incident.

2. If yes, what should be the minimum requirements such risk preparedness plans should comply with? For instance, should they:

- **Explain the various types of risks?**
- **Identify the demand side measures Member States plan to take (e.g., use of interruptible contracts, voluntary load shedding, increased efficiency, energy savings)?**
- **Identify the supply side measures Member States plan to take (e.g., increased production flexibility, increased import flexibility)?**
- **Assess the expected impact of existing and future interconnections?**
- **Identify roles and responsibilities?**
- **Identify how Member States co-operate or intend to co-operate amongst each other to identify, assess and mitigate risks?**
- **Other elements?**

The risk preparedness plan should be based on an existing risk assessment methodology. A great number of methodologies exist today, but all usually follow the same basic process:



The different possible remedial actions should be classified based on the time needed to implement them. Increasing energy efficiency is a long-term remedial action to counter scarcer energy resources; interruptible contracts and voluntary load-shedding, however, are used when an incident occurs.

Assessing the impact of existing and future interconnections is also crucial, but requires coordination between Member States: any major incident occurring in one electricity network has the potential to spread over neighbouring networks. Also, if an incident occurs, a Member State may not be able to rely on all its interconnectors.

These plans should also include simulation and training procedures for all relevant parties.

3. Do you think that it would be useful to establish a common template for risk preparedness plans?

Yes, defining or selecting a common methodology for risk assessment would help Member States and companies to coordinate across borders and to base their mitigation actions on a shared understanding of risks.

4. Given that electricity markets are increasingly interlinked, should risk preparedness plans be prepared at the national, regional or EU level?

Due to the increasing number of interconnections between EU Member States, these plans should be prepared at European, regional (probably synchronous area level) and national level.

5. Do you see a role for the Commission in assessing these plans? Would you see an added value of having the plans peer reviewed, at a regional or EU level? What role do you see in this context for the Electricity Coordination Group?

The European Commission should keep track of the plans, ensure they are aligned with the chosen methodology and ensure they are delivered on time. When it comes to assessing the content of these plans, national ministries, TSOs and DSOs should peer review them. This peer-review process may be coordinated by the EC.

In that context, the Electricity Coordination Group might be an appropriate forum, provided that it opens its membership to DSO representatives.

6. What level of transparency should be given to the plans? Who should be informed of what?

The risk assessment methodology should be made public; however, access to the plans themselves should be limited to Member States, TSOs, DSOs and other relevant parties.

7. How often should risk preparedness plans be made / be updated? What are the relevant time frames to be covered?

Risk preparedness plan should be updated on a regular basis and at least every five years, as proposed in the draft Emergency and Restoration network code[1]. This timeframe could be reduced to two or three years when the installed capacity of renewable energy sources (RES) grows and requires network companies to reshape and adapt their networks.

8. Given the challenges that DSOs are facing (e.g. integration of renewables, more decentralised systems), should DSOs take an active participation in the assessment of the risks and preparation of the risk preparedness plans? If yes, do you see the need for separate assessments and separate risk plans at the DSO levels? Or do you believe it is more appropriate to ensure an active participation of DSOs in risk assessments and risk preparedness plans covering the entire electricity system?

Today, most European DSOs operate high-voltage, medium-voltage, and low-voltage networks, and connect a majority of RES. Their impact on, and responsibility towards, overall system stability is high. For this reason, it does not seem appropriate to produce separate assessments and separate risks plans at the DSO level.

On the contrary, a set of well-articulated risk preparedness plan -- at national, regional and EU-level – is needed to cover the entire electricity system.

[1] Text issued by ENTSO-E on 25/03/2015 (https://www.entsoe.eu/Documents/Network%20codes%20documents/NC%20ER/150325_ENTSO-E_NC%20ER_final.pdf)

9. Ensuring cybersecurity is an increasingly important aspect of security of supply. What measures should Member States take to protect themselves against possible cyber-attacks or other cyber-related threats? Do you see the need for specific EU rules on cyber security, targeted to the energy field? Given the cross-border nature of cyber security risks, what scope is there for enhancing co-operation (for instance through the exchange of best practices)?

Member States should define their own national cybersecurity strategy (if not done already) and exchange knowledge regarding current threats and potential remedial actions. Most Member States have already set up their own computer emergency response teams (CERT) which are in contact with TSOs, DSOs and other operators of critical infrastructures.

It would appear, however, that cross-border cooperation is limited. The swift adoption of the network information security directive could help boost cooperation between Member States, provided its content remains ambitious enough.

With regards to the energy sector, additional rules are not necessary. There are specific cybersecurity requirements currently being addressed by DSOs relating to safe operation of the networks, as well as secure and private delivery of data to third parties

Nevertheless, a dedicated knowledge sharing platform at the EU-level could prove beneficial for the industry. The ground work for such platform is already being done by the EU-funded project "DENSEK" (www.densek.eu). If its results are positive, this project could be continued under another form after its conclusion.

Addressing crisis situations

10. Currently, it appears that in some Member States, detailed emergency plans exist, whereas in others, there are only very summary emergency plans. Should there be an obligation for all Member States to plan for crisis situations, e.g., by including relevant rules and measures in the overall risk preparedness plans?

Member States should draw plans for crisis situations, together with the energy industry. There might not be any need to add these requirements to risk preparedness plan, however, as the draft Emergency and Restoration network code already describe them at length.

11. If yes, what should be the minimum requirements to be included? For instance, should Member States be required to:

a) **Identify actions and measures to be taken in emergency situations (market and nonmarket- based)?**
b) **Set out the conditions for suspension of market activities?**

c) **Identify categories of 'protected customers' which, in case of a crisis, should not be subject to a disconnection measure (or only be disconnected by way of a last resort)?**
d) **Establish rules for cost compensation?**
e) **Indicate how they intend to co-operate with other Member States?**
f) **Reflect any other issues in their plans?**

As mentioned above, the draft Emergency and Restoration network code, will require TSOs, DSOs and other relevant stakeholders to:

1. Identify actions and measures to be taken (chapter 1 and 2)
2. Respect certain conditions for markets suspension (article 33 and 34)
3. Identify protected customers that should not be part of load-shedding plans or should recover supply in priority (Article 9.2.c)
4. Define TSO cooperation rules across borders (article 12 and Chapter 5).

Rules for cost compensation, if any, will have to be drafted by national regulatory authorities (NRAs). Adding new requirements related to emergency and restoration to the risk preparedness plan seem redundant with this forthcoming adoption and implementation of this network code.

Roles and Responsibilities

12. In relation to risk preparedness, how do you see the roles and responsibilities of:

- **National governments**

Drafting of national risk preparedness plan, reviewing them in coordination with all stakeholders and monitoring compliance.

- **NRAs**

Assessing the coherence of the plan vis-à-vis existing national energy regulation. Giving an opinion on potential changes to the plan or potential changes to the legislative framework, if necessary.

- **TSOs**

Drafting emergency and restoration plan together with DSOs. Executing the plan in coordination with DSOs and neighbouring TSOs.

- **DSOs**

Drafting emergency and restoration plan together with the TSO. Executing the plan in coordination with neighbouring DSOs and with the TSO.

- **European bodies such as ENTSO-E, ACER, and the Electricity Coordination Group**

Contributing to the peer review of the plans.

- **European Commission**

Verify that Member States prepare risk preparedness plans and coordinate the drafting/selection of the risk assessment methodology.

- **Other stakeholders, such as consumers**

In case a clear risk to security of supply is identified in one Member State, consumers should be made aware of that risk and invited to take preventive actions or change their energy consumption habits.

13. Given the fact that many actors are concerned by security of supply issues, would you see an added value in the designation by each Member State of a 'Competent Authority', responsible for coordinating security of electricity supply issues at national level?

The creation of an additional entity on top of national ministries, NRAs, TSOs and DSOs is not necessary. Selecting one organisation and giving it a coordination role, however, could be useful, if deemed appropriate in some Member States.

14. If it is decided to strengthen regional co-operation on a more structural basis between various players (e.g., when drawing up risk preparedness plans), how should regions best be defined?

Regions should be defined taking into account cross-border interconnection capacity, generation mix, and grid technical settings such as protection types. To avoid creating multiple and overlapping "regions" for different aspect of system operation, EDSO suggests using the LFC blocks mentioned in the draft Load Frequency Control and Reserves (LFCR) network code[2].

[2] Text issued by ENTSO-E on 28/06/2013
(https://www.entsoe.eu/fileadmin/user_upload/_library/resources/LCFR/130628-NC_LFCR-Issue1.pdf)

EDSO for Smart Grids is a European association gathering leading electricity distribution system operators (DSOs), cooperating to bring smart grids from vision to reality.

www.edsoforsmartgrids.eu