Joint ACER-CEER response to the European Commission's consultation on risk preparedness in the area of security of electricity supply

8 October 2015

Introduction

CEER and ACER welcome the opportunity to provide comments to the European Commission's consultation on risk preparedness in the area of security of electricity supply. As a general remark, we note that the scope of risk preparedness as addressed in this consultation may potentially overlap with some specific solutions proposed in the Network Code on Emergency and Restoration as well as with the issues addressed within the scope of Critical Infrastructure Protection. Therefore, we call for a close coordination of those aspects, ensuring all elements are consistently covered.

Question 1, 2 and 3

We believe that even though the Electricity Security of Supply Directive 2005/89/EC[1] does not require Member States (MSs) to draw up a risk preparedness plan, a majority of MSs address the issue in some form; this is also valid for emergency plans. Therefore, we would find it useful to prepare an inventory of how the issue is currently addressed within MSs. This implies the determination of current roles and responsibilities including associated legislative levels. Following this exercise, the relationship with the processes foreseen pursuant to the Network Codes on System Operation and the European Critical Infrastructure Protection (EPCIP) needs to be established. A gap analysis should help identify problems that would benefit from implementation of European policy options.

We note that some items proposed under question 2 (such as supply side measures or impact of interconnectors) seem to be very detailed and would possibly be addressed within national System Defence Plans prepared pursuant to the System Operation Network Codes.

Question 4

We believe that different elements of risk preparedness plans may be elaborated at EU or MS levels, whereas their level of detail should be increasing towards the MS level due to the growing importance of local specificities. We also note that the System Operation Network Codes include explicit roles for Regional Security Coordinators (RSCs) and that these could be chosen in the future to foster the identification of relevant risks and of preventive measures more efficiently on a regional basis, acting collectively, than by individual MSs.

[1] Directive 2005/89/EC of the European Parliament and of the Council of 18 January 2006 concerning measures to safeguard security of electricity supply and infrastructure investment (Text with EEA relevance).

Question 6

Bearing in mind that risk preparedness plans in the energy sector address critical infrastructure, and are therefore of a highly sensitive nature, the detailed plans should only be available to those persons and organisations directly affected.

Question 7

Risk preparedness plans should be updated regularly - upon changes in the system which significantly affect the underlying assumptions or upon lessons learned.

Question 8

Bearing in mind different national structures (e.g. number of DSOs ranging from a few to several hundred), a single role for the DSO's involvement in preparation of plans may be difficult to implement. Nonetheless, plans need to foresee implementation measures which may go down to the level of DSOs (e.g. on cyber security, demand side response or distributed generation).

Question 9

In view of existing frameworks and guidelines[2] as well as current activities by the European Commission, it is believed that the forthcoming Network and Information Security Directive (NIS)[3] as well as the General Data Protection Regulation (GDPR)[4] should be the prime legal documents in the area of cybersecurity. The forthcoming Directive and Regulation should be applicable for all providers of critical infrastructure and should, where possible, include precise rules for the energy sector.

In this regard, CEER believes that a comprehensive initiative targeted to promoting cross-border cooperation led by the European Commission and backed by national governments could significantly enhance cooperation and augment the EU's overall resilience to cyber-threats.

[2] i.e. Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection; the Cyber Security Strategy of the European Union (JOIN/2013/1 final); the policy on Critical Information Infrastructure Protection (CIIP) COM (2009/149 final); and the Digital Agenda for Europe (COM/2010/0245 final).

[3] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (COM(2013)0048- C7-0035/2013-2013/0027 (COD)).

[4] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

Question 10 and 11

The current drafts of the System Operation Network Codes already address issues listed in question 11 at the level of TSOs. The Network Code on Emergency and Restoration (NC ER) obliges each TSO to prepare a System Defence Plan and specifies (Article 9) which elements it shall include and which principles it shall follow. As such, it provides a harmonised framework for development of national plans and, consequently, those plans should be sufficient to cover crisis situations. The NC ER also requires the development of rules, including conditions, for market suspension and market restoration (chapter 4). The Network Code on Operational Security obliges TSOs to prepare Business Continuity Plans and covers identification of high priority customers, whose list should be approved by each NRA.

The System Operation Network Codes do not address the cooperation among MSs, nor do they cover cost compensation. Nevertheless, in case of emergency, technical aspects (quickly restoring the secure state) should have priority over financial aspects. A solidarity principle should be applied when it comes to blackout prevention.

Question 5, 12 and 13

There are different roles assigned to all listed levels, e.g. MSs are responsible for policy directions (both EU based via network codes and nationally); while TSOs prepare and implement specific measures fulfilling those policies. These roles should be defined consistently at the higher level – the Electricity Coordination Group (ECG) may provide an interlinkage between technical and political/economical aspects.

Given their neutrality and regular interface with MSs, TSOs and public (consumers' interests), the coordinating role for security of supply issues should be assigned to NRAs.

However, if the gap analysis mentioned in answer to questions 1, 2 and 3 so identifies, the roles and responsibilities could be harmonised across the EU so as to improve the efficiency of the decision making process in case of cross-border system design and operation issues. All NRAs could be assigned with approval powers of the system operation related methodologies and coordinate such approvals under ACER umbrella.

Question 14

Given the framework provided by System Operation Network Codes for establishing Regional Security Coordinators (RSC), and keeping in mind ACER's recommendation that RSCs should be involved in offline and close-to-real time coordination of emergency state, the geographical perimeter for risk preparedness plans should be aligned with the geographical perimeter of RSCs.