Regulatory Frameworks for Cyber Security in the Electricity Sector: the European path

G. Dondossola

Web – 24 march 2021
1. By 9 November 2018, for each sector and subsector referred to in Annex II, Member States shall identify the operators of essential services with an establishment on their territory.

- Energy: Electricity, Oil, Gas;
- Transport: Air transport, Rail transport, Water transport, Road transport;
- Banking;
- Financial market infrastructures;
- Health sector;
- Drinking water supply and distribution;
- Digital Infrastructure: Internet Exchange Points, DNS service providers, Top Level Domain name registries.
2. The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows:

(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
(b) the provision of that service depends on network and information systems; and
(c) an incident would have significant disruptive effects on the provision of that service.
1. When determining the significance of a disruptive effect as referred to in point (c) of Article 5(2), Member States shall take into account at least the following cross-sectoral factors:

(a) the number of users relying on the service provided by the entity concerned;
(b) the dependency of other sectors referred to in Annex II on the service provided by that entity;
(c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;
(d) the market share of that entity;
(e) the geographic spread with regard to the area that could be affected by an incident;
(f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.
1. Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority.
1. Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations.

2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.
3. Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.
1. The European cybersecurity certification framework shall be established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonised approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services and ICT processes.
Article 52 Assurance levels of European cybersecurity certification schemes

1. A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services and ICT processes: ‘basic’, ‘substantial’ or ‘high’. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident.
EUCC candidate certification scheme

Cybersecurity Certification: EUCC Candidate Scheme — ENISA (europa.eu)

- published by ENISA on July 2020
- based on Common Criteria (ISO/IEC 15408 and ISO/IEC 18045)
Network Codes and Data Exchanges
European Electricity Sector

The code families

**Connection**
- Requirements for Generators
- High Voltage Direct Current Connections
- Demand Connection Code

**Operations**
- Operations
- Emergency and Restoration

**Market**
- Forward Capacity Allocation
- Capacity Allocation & Congestion Management
- Electricity Balancing
Network Code on Cybersecurity

ENTSO-E / EU DSO Draft – NC structure

ENTSO-E / EU-DSO working group (consulting relevant stakeholders)

- Cross-border cyber risk assessment and management
  - Risks to be mitigated

Individual TSOs and DSOs

- ISO/IEC 27001 certification
  - Mandatory controls in SoA (ISO/IEC 27019)
  - Technical guidelines on the implementation of controls

European energy sector CSIRT

- Sharing of technical information

Figure 4: NC Structure

Second Interim Report

Recommendations for the European Commission on a Network Code on Cybersecurity

31 October 2020
Network Code on Cybersecurity

ENTSO-E / EU DSO Draft – certification process

- Unified requirements for certification bodies & Auditors
- Requirements for professional knowledge
- Audit focus

Second Interim Report

Recommendations for the European Commission on a Network Code on Cybersecurity

31 October 2020

The mission of the Drafting Team is to prepare the ground for a future Network Code on Cybersecurity for the electricity sector.
Common Security Controls

1. Identify the common critical business processes of the European Energy System
2. Identify the security risks of the common critical business processes

3. TSO’s / DSO’s must implement the minimum set of common security controls (and additional controls for specific risks)
4. Select the controls for identified security risks (minimum set of security controls)
5. TSO/DSO setting additional security requirements
6. System integrators
7. Vendors

Figure 7: Process to use the common security controls
Network Code on Cybersecurity

ENTSO-E / EU DSO Draft – NC structure

ENTSO-E / EU-DSO working group (consulting relevant stakeholders)

- Cross-border cyber risk assessment and management
  - Risks to be mitigated

Individual TSOs and DSOs

- List of critical processes (scope)
- Risk assessment (acceptance) criteria

ISO/IEC 27001 certification

- Mandatory controls in SoA (ISO/IEC 27019)
- Technical guidelines on the implementation of controls

Common security controls and requirements

- Product requirements

Product assurance scheme

European energy sector CSIRT

Sharing of technical information

Second Interim Report

Recommendations for the European Commission on a Network Code on Cybersecurity

31 October 2020

The mission of the Drafting Team is to prepare the ground for a future Network Code on Cybersecurity for the electricity sector.
Sources

8. Clean Energy for all Europeans Package, European Union 2019
Thank you
Giovanna.Dondossola@rse-web.it