WP-042-2021

Response to the ACER consultation on the framework guidelines

Version 1.0

21 June 2021

This document is shared under the Traffic Light Protocol classification:

TLP WHITE - public

The European Network for Cyber Security (ENCS) is a non-profit membership organization that brings together critical infrastructure owners and security experts to deploy secure European critical energy grids and infrastructure. Founded in 2012, ENCS has dedicated researchers and test specialists who work with members and partners on applied research, defining technical security requirements, trainings, and component and end-to-end testing.

ENCS

Response to the ACER consultation on the framework guidelines

On April 31, ACER published draft framework guidelines [1] for the network code on cyber-security as part of a public consultation. The draft framework guidelines set the general principles the network code should meet. They build on the previous work from the Smart Grid Task Force Expert Group 2 [2] and the informal drafting team from ENTSO-E and the four DSO associations (CEDEC, E.DSO, Eurelectric, and GEODE) [3].

The draft framework guidelines help to clarify the governance for the network code and give some new ideas for its rules. But they make different choices from the recommendations of the informal drafting team in several major areas. In some of these choices, we think that the draft framework guidelines are overlooking practical considerations of the informal drafting team. We think these choices will lead to substantial extra costs, not in proportion to the gains in security.

We therefore think the network code should aim for rules that are more practical to implement. In particular, it should:

- determine the scope of the advanced measures through processes
- set lower minimum security requirements for important undertakings
- require essential undertakings to have a management system
- set the minimum requirements in terms of security controls
- allow alternative assurance methods besides product certification
- require SOC functions only for essential processes

Determine the scope of the advanced measures through processes

We think that the part of the organization that is considered essential should be determined through processes rather than assets. The draft framework guidelines propose to first make an inventory of all assets, and then determine which assets are essential through a risk assessment. This would mean many assets will be identified and analyzed that are not essential to cross-border electricity flows. The unnecessary analysis creates extra costs and keeps scarce security experts tied up. Taking measures to improve security will be delayed until the asset inventory is completed, which could take years.

The detailed asset inventory is moreover strictly confidential. It cannot easily be shared when doing the cross-border risk assessment. Regulators would have to take extra security measures to handle the information.

It would be more efficient to start top-down and first determine on a European level which processes are needed to ensure cross-border electricity flows. From this it can be determined which processes are essential at the undertaking level. Then the electricity undertakings can determine the assets they need to support these processes. Working in this way, the effort can be focused on only the essential assets, leading to a more cost-effective reduction of security risks. Critical issues would be addressed much faster. Moreover, only the electricity undertaking itself would need to have the full asset inventory.

The top-down, process-based approach should also be used for the cross-border risk assessment. The draft framework guidelines proposes that the risk assessments of individual undertakings are first combined at members state level by the National Competent Authorities, and then at regional level by Regional Coordination Centers. In bottom-up approach, it is easy to get overwhelmed with the details. Member states would get opinions from tens or hundreds of different undertakings, all with their own interests and risk assessment methods. A top-down approach has the advantage that the analysis can quickly focus on the processes that are most important for the European electricity grid.

Set low minimum security requirements for important entities

We think it is better to set lower security requirements for important entities. In the draft framework guidelines, any electricity undertaking that is not a small or micro entity is considered at least an important entity, and hence must meet the minimum security requirements. These minimum requirements are quite high. They include implementing the principles in the standards matrix (EPSMM) and setting up SOC activities. With so many organizations having to implement the minimum requirements, it would be more reasonable to set the minimum security requirements close to the basic cyber security hygiene requirements for small and micro enterprises.

The main reason for setting lower minimum requirements would be to avoid unnecessary costs. It is of course advisable that every electricity undertaking does their own cybersecurity risk assessment and takes appropriate security measures. But they should not be forced to take measures by the network code if they do not form a risk to the European electricity grid.

Another reason to set lower requirements, is that the broad scope proposed in the draft framework guidelines will make it hard for regulators to effectively enforce the network code. Many regulators are still working to set up proper oversight for the TSOs, DSOs, and producers identified as essential under the NIS directive. In two years, they would suddenly have to monitor many additional and highly diverse undertakings.

Require essential undertakings to have a management system

We think that the network code should require essential electricity undertakings to have a management system for cybersecurity. The draft framework guidelines contain elements of a management system, such as performing as risk assessment and implementing security controls. But they leave out the internal feedback loop (“plan-do-check-act cycle”) in which organizations look for problems in the effectiveness of controls and fix them.

Such a loop is needed to ensure that essential undertakings maintain their target level of security in the long run. In any larger organization there will be problems in implementing controls. Policies will not always be followed, or they may not achieve their intended goals. Incidents may show that important controls were missing. Electricity undertakings must have a structural way to deal with such problems, and to involve management to ensure resources are available for this.

The maturity model approach stressed in the draft framework guidelines can be a useful tool within a management system. But we do not think the approach is ready to be used on its own. Management systems have been applied for many years and are already used in the NIS directive implementation in many countries. Maturity models are used at a much smaller scale and in a less formal setting. It is a major risk to make them the core of mandatory regulation affecting thousands of undertakings in the electricity sector.

We do think the ACER proposal to consider national obligations as equivalent to certification strikes a good balance. Certification would bring more harmonization and would likely be more cost-effective in the long term. But many TSOs and DSOs have made major investments to comply to the NIS directive. It would be wasteful not to use these investments. To ensure European harmonization, national regulators should show that the national obligations are at the same level as the security controls selected by ENTSO-E and the EU-DSO entity.

Set the minimum requirements in terms of security controls

We think ENTSO-E and the EU-DSO entity should develop the security requirements for important and essential undertakings as a minimum set of controls. The draft framework guidelines propose that they develop a matrix that maps all relevant standards to security principles. This approach seems unnecessarily complex.

ENTSO-E and the EU-DSO entity would first have to create the list of principles, consulting all relevant stakeholders and following a formal approval process involving ACER, ENISA, and the European Commission. This work would be just reinventing the wheel, as there are already mature and widely accepted sets of principles underlying

international standards, such as ISO/IEC 27001, IEC 62443 or the NIST cybersecurity framework.

Mapping all relevant standards to the principles would also be considerable work for ENTSO-E and the EU DSO entity. They would have to track all relevant international standards and national regulation in all involved member states. Objectively mapping all controls from these standards to maturity levels would take extensive analysis. And there could be pressure to allow some standards that technical experts find lacking in certain areas.

We do not think all this work will lead to the desired harmonization on a minimum security level. As all national regulations would be in the matrix, the approach will run into the same harmonization problems as the NIS directive.

Allow alternative assurance methods besides product certification

We think that the network code should allow electricity undertakings to use alternative assurance methods besides product certification. The draft network code now asks to make EU Cybersecurity Certification schemes (as defined in the Cybersecurity Act [4]) mandatory by 2027 at the latest. But mandatory certification is not needed to improve security or cost-effectiveness and will force essential undertakings to use certification in cases when it makes no sense.

Regulators can ensure that essential undertakings acquire secure products and systems using the approach proposed by the informal drafting team. The approach requires essential undertakings to manage their risk and take minimum controls for secure acquisition. The controls can require that essential undertakings either use certified products or systems or do their own assurance with the same coverage and depth. So, allowing alternative assurance methods will not lead to less security.

Making product certification mandatory is also not needed to improve cost-effectiveness. Product certification can be cost-effective if it is implemented well. Tests only need to be performed once, not by every electricity undertaking who uses the product. And suppliers face a harmonized market for security, so that they can focus their security investments. But if it is cost-effective, electricity undertakings will start procuring certified products voluntarily, as they notice that doing so costs less than doing their own assurance.

Mandatory certification may actually increase costs, as it will force electricity undertakings to use certified products even when this is not cost-effective. They would have to get products that are customly developed for them certified, even when no one else will use them. And they would have to use it for products and systems for which no suitable scheme is yet available. We cannot know now for which products good schemes will be available in 2027. So, we cannot restrict the network code to such products.

Allowing equivalent alternative assurance methods allows electricity undertakings to do their own assurance when certification is too costly, while still providing a strong incentive to use certified products whenever a cost-effective scheme is available.

Require SOC functions only for essential processes

We think that the network code should only require SOC functions for essential processes. The draft framework guidelines recommend requiring them for all important entities. But SOC functions carry significant costs in personnel, training, and software. It does not seem proportional to require them for such a broad scope.

Moreover, having to monitor everything takes the focus away from essential systems. Analysts would spend most of their time on incidents in web-facing systems or office systems. They would spend little time on operational technology systems, in which there are few incidents. But these systems are essential to the electricity grid.

We also think that the network code should not make requirements on how the SOC functions are organized. It should specify what activities an essential undertaking must perform, such as intrusion detection, incident response and vulnerability management. But it should not specify that these should be performed by a separate organizational unit, such as a SOC. Each undertaking should be allowed to choose the organizational model that fits them best.

References

[1] ACER, „Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows (Draft),” 30 April 2021.

[2] Smart Grid Task Force Expert Group 2, „Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management,” 2021.

[3] Network code on cybersecurity - Informal drafting team, „Final report: Recommendations for the European Commission on a Network Code on cybersecurity,” 2021.

[4] The European Parliament and the council of the European Union, „Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act),” 2019.