European Network of
Transmission System Operators
for Electricity
entsoe

Position paper on the European Commission’s proposal for a Cyber Resilience Act

Final | 6 June 2023

From: Information & Communication Technologies Committee

ENTSO-E Mission Statement

Who we are

ENTSO-E, the European Network of Transmission System Operators for Electricity, is the association for the cooperation of the European transmission system operators (TSOs). The 39 member TSOs, representing 35 countries, are responsible for the secure and coordinated operation of Europe's electricity system, the largest interconnected electrical grid in the world. In addition to its core, historical role in technical cooperation, ENTSO-E is also the common voice of TSOs.

ENTSO-E brings together the unique expertise of TSOs for the benefit of European citizens by keeping the lights on, enabling the energy transition, and promoting the completion and optimal functioning of the internal electricity market, including via the fulfilment of the mandates given to ENTSO-E based on EU legislation.

Our mission

ENTSO-E and its members, as the European TSO community, fulfil a common mission: Ensuring the security of the inter-connected power system in all time frames at pan-European level and the optimal functioning and development of the European interconnected electricity markets, while enabling the integration of electricity generated from renewable energy sources and of emerging technologies.

Our vision

ENTSO-E plays a central role in enabling Europe to become the first climate-neutral continent by 2050 by creating a system that is secure, sustainable and affordable, and that integrates the expected amount of renewable energy, thereby offering an essential contribution to the European Green Deal. This endeavour requires sector integration and close cooperation among all actors.

Europe is moving towards a sustainable, digitalised, integrated and electrified energy system with a combination of centralised and distributed resources. ENTSO-E acts to ensure that this energy system keeps consumers at its centre and is operated and developed with climate objectives and social welfare in mind.

ENTSO-E is committed to use its unique expertise and system-wide view – supported by a responsibility to maintain the system's security – to deliver a comprehensive roadmap of how a climate-neutral Europe looks.

Our values

ENTSO-E acts in solidarity as a community of TSOs united by a shared responsibility.

As the professional association of independent and neutral regulated entities acting under a clear legal mandate, ENTSO-E serves the interests of society by optimising social welfare in its dimensions of safety, economy, environment, and performance.

ENTSO-E is committed to working with the highest technical rigour as well as developing sustainable and innovative responses to prepare for the future and overcoming the challenges of keeping the power system secure in a climate-neutral Europe. In all its activities, ENTSO-E acts with transparency and in a trustworthy dialogue with legislative and regulatory decision makers and stakeholders.

Our contributions

ENTSO-E supports the cooperation among its members at European and regional levels. Over the past decades, TSOs have undertaken initiatives to increase their cooperation in network planning, operation and market integration, thereby successfully contributing to meeting EU climate and energy targets.

To carry out its legally mandated tasks, ENTSO-E's key responsibilities include the following:

› Development and implementation of standards, network codes, platforms and tools to ensure secure system and market operation as well as integration of renewable energy;

› Assessment of the adequacy of the system in different timeframes;

› Coordination of the planning and development of infrastructures at the European level (Ten-Year Network Development Plans, TYNDPs);

› Coordination of research, development and innovation activities of TSOs;

› Development of platforms to enable the transparent sharing of data with market participants.

ENTSO-E supports its members in the implementation and monitoring of the agreed common rules.

ENTSO-E is the common voice of European TSOs and provides expert contributions and a constructive view to energy debates to support policymakers in making informed decisions.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Having products with digital elements that have strong cybersecurity requirements is the key to mitigate cybersecurity risks in the long term, thus, the proposed Cyber Resilience Act (henceforth CRA) will be a major step in improving product security. While the CRA lays down direct obligations only for manufacturers, importers, and distributors, it also seeks to improve the security of critical infrastructures by setting stricter conformity assessment requirements for critical products. For TSOs, as operators of critical infrastructure, it is, therefore, crucial that the CRA is designed in a way that optimally supports TSOs to mitigate cybersecurity risks and is coherent with other relevant EU legislations which aim to ensure cybersecurity of critical infrastructure.

In this respect, besides the CRA, TSOs will need to comply with two other EU cybersecurity legislations that address the cybersecurity of products: the *Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148* (henceforth NIS2 Directive), and the upcoming *Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows* (henceforthNCCS). The CRA should be aligned with both EU legislations, so that scarce cybersecurity resources are used most efficiently.

The CRA is already well aligned with the NIS2 Directive. Nevertheless, ENTSO-E believes that the alignment with the NCCS can be improved based on the proposals mentioned below.

ENTSO-E's recommendations

The CRA should be aligned with the NCCS by:

- adopting requirements developed under the NCCS as sectoral rules under the CRA;
- using the results from the NCCS regional cybersecurity risk assessment for the electricity sector to determine which products are critical;
- requiring manufacturers to consider the results from the NCCS regional risk assessment in the risk assessments they need to perform under the CRA.

Additionally, for the CRA to support cybersecurity risk mitigation for TSOs, more transparency should be provided to users regarding which risks a product can mitigate.

ENTSO-E's recommendations

The Cyber Resilience Act should provide more transparency to users of critical products by:

- requiring manufacturers to describe the threats mitigated in the user documentation;
- requiring manufacturers to describe the assurance level in the user documentation;
- defining clear criteria for when a reassessment needs to be performed for a product.

INTRODUCTION

On 15 September 2022, the European Commission (henceforth the EC) published a *Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*, known also the CRA. The proposal includes far-reaching provisions on product security. All products with digital elements must meet certain essential cybersecurity requirements, covering both technical security measures and patching. For critical products, these requirements must be verified by independent testing and product certification.

The CRA could be highly useful for TSOs by raising the security of products with digital elements used in critical infrastructure, such as the electricity transmission grid. TSOs are purchasing many of their equipments for substations or control centres, metering devices and industrial IoT from external suppliers. Taking into account previously mentioned information, a good baseline security is achieved if such products meet the essential security requirements. Moreover, the accelerated digitalisation of different economic sectors and the electrification of demand in the industry, construction, mobility and heat sectors means that products with digital elements will be connected at a lower voltage levels of the electricity grid. Thus, a well-designed CRA will not only support high-level of cybersecurity for the transmission grid but for the electricity sector in general.

TSOs, however, also need to apply to other EU cybersecurity legislation which are aimed at operators of critical infrastructure and essential entities. Specifically, TSOs will need to meet the NIS2 Directive (already in force, and to be transposed by Member States by October 2024) and the upcoming NCCS. To ensure that all these cybersecurity regulations work well together, ENTSO-E has produced this analysis and recommendations for the CRA.

ALIGNMENT WITH THE NETWORK CODE ON CYBERSECURITY

Besides the proposed CRA, TSOs will need to comply with two other EU legislations addressing the cybersecurity of products with digital elements:

1. the *Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148* (NIS2 Directive), and

2. the *Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows* (NCCS) - upcoming.

It is crucial that the CRA is aligned with both regulations mentioned above. The consequences of non-alignment might lead to the scarce cybersecurity resources available to TSOs and suppliers being used inefficiently in order to comply with redundant or,possibly, contradictory rules on product security.

The CRA has clearly already been aligned with the NIS2 Directive. This is explained in the section on the interplay with existing policy provisions of the CRA proposal by the EC. In Article 2, the CRA also references sectoral legislation for medical devices (Regulation (EU) 2017/745 and 2017/746), motor vehicles (Regulation (EU) 2019/2144), and civil aviation (Regulation (EU) 2018/1139). The CRA, however, does not reference the NCCS as a sectoral rule for the electricity sector.

In the opinion of ENTSO-E, the NCCS should be referenced as a relevant EU sector legislation. The work that will be performed for the NCCS should be used to strengthen the implementation of the CRA in the electricity sector in three ways:

- if suitable requirements are developed as part of the procurement recommendations from the NCCS, these should be used as sectoral rules under Article 2(4) of the CRA. In particular Articles 24 and 25 in the ACER revised NCCS referring to the Common Electricity Cybersecurity Framework and the Minimum and Advanced Cybersecurity Supply Chain Security Controls should be considered;

- the outcomes of the regional cybersecurity risk assessment performed under the NCCS should be used to divide products specific to the electricity sector into class I, class II, and high critical products. Article 20 of the ACER revised NCCS foresees the production of the regional cybersecurity risk assessment within 30 months after the start of each risk assessment cycle;

- Manufacturers should be required to consider the threats identified under the NCCS regional cybersecurity risk assessment when performing their risk assessment under Article 10 (2).

Using the NCCS procurement recommendations as sectoral rules

ENTSO-E recommends that if suitable requirements are developed under the NCCS, these should be adopted as sectoral rules or Delegated Acts.

The NCCS (ACER revised version) tasks ENTSO-E, in collaboration with the EU DSO Entity, to develop procurement recommendations for ICT products, services, and processes. Together, ENTSO-E and the EU DSO Entity will set up a rolling work programme to develop such recommendations for ICT products, services, and processes that can have a high or critical impact on the electricity grid. The impact is determined through the regional cybersecurity risk assessment performed for the NCCS. Users of the products in the electricity sector will be involved in the programme through extensive Stakeholder consultations.

As part of the procurement recommendations, ENTSO-E and the EU DSO Entity intend to develop harmonised security requirements. The goal is to develop requirements for products specific to the electricity sector. These products will likely include the Industrial Automation & Control Systems (IACS), Industrial Internet of Things devices, and smart meters as mentioned in the CRA.

The requirements developed under the NCCS will be designed to counter the cybersecurity risks to the electricity system, as identified in the NCCS cybersecurity risk assessments. These requirements will also take into account the specific constraints of the sector, such as, the need of products to meet real-time requirements. The NCCS requirements, hence, would be a good basis for implementing the essential cybersecurity requirements of the CRA. In particular, Articles 24 and 25 in the ACER revised NCCS referring to the Common Electricity Cybersecurity Framework and the Minimum and Advanced Cybersecurity Supply Chain Security Controls should be considered as starting point.

One proposal on how to use the NCCS requirements would be to turn them into harmonised standards. However, it would bring more gravity if these requirements for key products would become mandatory for manufacturers. This would be useful for Industrial Automation & Control Systems (henceforth IACS) used in the electricity sector, including supervisory control and data acquisition systems (henceforth SCADA), energy management systems (henceforth EMS),and industrial equipment at electrical substations.

If sectoral rules apply, Article 2 (4) of the CRA proposal permits products to be excluded through a Delegated Act.. This provision may, however, not be applicable to the future NCCS requirements, as these are not mandatory for the Delegated Act stemming from the Electricity Regulation 943/2019. Therefore, ENTSO-E believes that a mechanism should be found in order to turn non-mandatory sectoral rules, such as those in the current ACER revised NCCS into a replacement of the essential security requirements for certain product types, for instance through Delegated Acts (Article 50).

NCCS should be explicitly referenced as a regulation providing sectoral rules. The CRA proposal already mentions sectoral regulations for medical devices and vehicles in point (12) and (13) of the related section. The NCCS should be similarly referenced.

Using the NCCS risk assessment to determine product criticality

The regional cybersecurity risk assessment performed under NCCS should be used for determining the criticality levels for products that are specific to the electricity sector. In this regard, Article 17 of the ACER revised NCCS, relating to Cybersecurity risk assessment methodologies which describes the risk impact matrix, would be useful for defining critical issues.

In the current CRA proposal, products are divided into class I and II in Annex III. No explicit rationale is provided that explains this division. For some products, the division does not match the perception of cybersecurity risks in the electricity sector. Class I, for instance, contains some product types that are critical to product OT systems of TSOs, such as identity management systems, VPN products, and remote access software.

It would be complex to execute the division into classes that is based on a risk assessment for all sectors involved. However, for products that are specific to the electricity sector, it would be feasible to consider the risks. The NCCS, as it is mentioned in its current version, will produce a regional cybersecurity risk assessment and a reference architecture for the electricity sector. Based on this work, it will be possible to identify which sector-specific products are most critical.

The electricity sector uses many sector-specific products in critical roles. Manufacturers are developing products specifically for electrical utilities, especially in the category of IACS and, in the future, for the category industrial internet of things (Examples are SCADA/EMS, and IEDs and RTUs for substations). For such products, there would be an added value in having a risk-based division.

The CRA empowers the EC to change the lists in Annex III through Delegated Acts (Article 6(3) and (5)). However, it is not certain how these Delegated Acts will reflect the specific requirements from sectors with critical infrastructure, such as the electricity sector, and, how these Delegated Acts will be aligned with relevant EU sector legislation such as the NCCS.

In the criteria for the classification listed in Article 6(2) of the CRA, it would be recommended to include the intended use of products by entities classified as high-impact or critical-impact entities under the future NCCS. A similar criterion is already included for essential entities under the NIS 2 directive (Article 6(2)(b)).

Requiring manufacturer to consider sectoral risks

The CRA proposal should require manufacturers of sector-specific products to consider sectoral risk assessments as an input for the risk assessment that they must perform according to Article 10 of the CRA proposal.

Article 10(3) already allows to use risk assessments performed under other acts for high-risk AI systems and medical devices. In this provision, ENTSO-E would like to advise to consider risk assessments made under the NCCS.

Manufacturers often do not have a full insight into the risks that users of their systems face. They do not know in which networks and systems their products are deployed. As they may not know what information is processed by their products, they cannot assess the possible impact on whether the products are being compromised. They may also lack insight into mitigating measures at system level, such as firewalls to shield critical systems.

Manufacturers would, hence, benefit from the information on risks that are being received from users. The ACER revised NCCS provides such information through the regional cybersecurity risk assessment. Current NCCS version states that the report will be prepared by ENTSO-E in cooperation with the EU DSO Entity through gathering of information from all high and criticalimpact entities in the electricity sector. It is currently being planned that there will be a declassified/public version of the report that will include a description of the main threats. If this information would be taking into account, it would help manufacturers to improve their risk assessments.,

MORE TRANSPARENCY FOR USERS OF CRITICAL PRODUCTS

The information and instructions to the userS should include more information on the risks mitigated and the tests performed in order to allow TSOs to select products with the right cybersecurity level.

ENTSO-E would like to advise to include this information as a part of the information and instructions to the users (listed in Annex II).

Under the NIS2 Directive and the current ACER revised NCCS version, TSOs will be required to manage their security risks. In order to do this, TSOs would require to know which risks they can mitigate with the security measures on the products. TSOs would also need to know the assurance level of the tests performed in the conformity assessment. For products used in critical systems, a high assurance level is needed.

Some information on these areas is provided in the information and instructions to the user, as described in Annex II of the draft CRA. Nevertheless, the information provided does not provide sufficient transparency in regards of the security properties of products for TSOs to meet their risk management obligations. TSOs will most likely need to organize their own cybersecurity testing on products. In order to avoid duplication and gain efficiency in protecting our critical energy network, ENTSO-E believes that it is essential to align the testing requirement in various legal proposals.

Transparency on the risks mitigated

The CRA should require manufacturers to provide users with more transparency on the risks that are mitigated by the security measures on the product. For critical products, the information and instruction to the user should include at minimum a list of threats mitigated, and a mapping of these threats to the security measures on the product.

TSOs need to understand the risks mitigated in order to meet their risk management obligations under the NIS2 Directive and the future NCCS as described below:

- according to NIS2 Directive, TSOs need to take appropriate and proportionate measures in order to manage the security risks of their network, services and information systems. TSOs only can decide on whether the cybersecurity measures implemented on a product are appropriate and proportionate, if they know which risks these measures are designed to protect against. They need to be able to compare the risk assessment that the manufacturer has performed under the CRA, against the risk assessment they themselves have performed under the NIS2 Directive;

- according to the ACER revised NCCS, TSOs need to set security requirements to products that they procure based on an entity-level risk assessment.. It is again useful to understand the risk assessment that the manufacturer has performed in order to check and ensure that a product meets these requirements

Under the CRA, the results of the manufacturer’s risk assessment for a product are shared with the notified body as a part of the technical documentation (Annex V, point 3). Nevertheless, the information and instruction to the user (Annex II) only provide information in regards of the intended use, and circumstances which may lead to a significant cybersecurity risks under the intended use or reasonably foreseeable misuse.

The information provided to users does not provide sufficient transparency in regards of security properties for critical infrastructure operators to perform their risk assessments, and, hence, to decide if a product is appropriate for their use. The CRA conformity assessment is then of limited value. TSOs and DSOs will still have to do their own testing of the product if they would really like to evaluate and understand the risks.

ENTSO-E believes that threat information is not too sensitive to share. It is a standard part of the information provided under existing cybersecurity certifications. For instance, it will be a part of the security targets for the European cybersecurity certification scheme (henceforth EUCC).

Transparency on the assurance level

The CRA should provide users with a transparency on the assurance level provided by the conformity assessment. For critical products, the information and instruction to the user should include a description of the tests performed as a part of the EU-type assessment or by the manufacturer as a part of their quality system for full quality assurance.

To know and evaluate which risks can be mitigated through a product, TSOs not only need to know that it meets the essential security requirements, they also need to know how thoroughly the product was evaluated by answering several question - did the supplier, for instance, do any penetration testing or code reviews? Or was the testing limited to documentation reviews or functional testing?

If the product was not tested thoroughly enough, TSOs will not have sufficient assurance that cybersecurity risks will be mitigated. Hence, they will need to order additional evaluation activities for the product.

The information and instructions to the users (Annex II) do not provide any information in regards of the assurance level. Possibly, the intention is that the CRA conformity assessment always provides a basic level of assurance, whilst the higher assurance levels will only be provided through the EU cybersecurity certification schemes of the Cybersecurity Act (Regulation (EU) 2019/881). However, this may be difficult to understand for users.

Misunderstanding in regards of the assurance level may lead to new risks as users place too much trust in the conformity assessment. If a declaration of conformity is available for a critical product, most users will assume that the product is secure enough to use in critical infrastructures. However, the conformity assessment may only include a review of the technical documentation. The assurance level then would be comparable to level 'basic' in the Cybersecurity Act. This would, in many cases, be too low for critical infrastructure use. In this way, the lack of transparency in the assurance level, could lead to a situation where products that have not been evaluated thoroughly enough are being used in critical functions.

Transparent criteria for reassessments

The CRA should provide clear rules on when a new conformity assessment needs to be performed, especially when EU-type examination (module B) is used.

Current cybersecurity certification schemes, such as Common Criteria, usually declare certificates valid for only the exact version of the product that was tested. Great amount of work is being done ,for instance, on the Common Criteria based on EUCC in order to allow for a quick recertification of updates that in turn would allow to avoid performing a full evaluation for every minor change. Nevertheless, defining rules for such recertification is a complex matter, as even small changes could introduce serious vulnerabilities.

The EU-type examination will face the same issue. Thereby, it should be made clear when a product is of the same type or when separate testing is needed. It seems reasonable that small updates would be considered of the same type and covered by the EU-type certificate. Clear rules should, however, be defined for when changes are so large that a new assessment is needed. Also, regular re-assessments should be required, for instance, every three years.

There also should be clear rules for when variant of the same product are considered the same type. TSOs, for instance, use several variants of the same industrial devices (e.g. Intelligent Electronic Devices (IEDs)) for which the security parts of the firmware are the same. The differences are in parts of the firmware that are not related to security. It would be reasonable to consider all these devices of the same type, so that they only need to be tested once. ENTSO-E believes, however, that there should be clear rules that ensure that the manufacturers would apply to this rule without stretching it too far.