bdew

Energie. Wasser. Leben.

BDEW Bundesverband
der Energie- und
Wasserwirtschaft e.V.
Reinhardtstraße 32
10117 Berlin
Telefon +49 30 300 199-0
Telefax +49 30 300 199-3900
E-Mail info@bdew.de
www.bdew.de

Statement

On the proposal for the EU Network Code on Cybersecurity

BDEW Comments on the first Deliverable of the Drafting Team

Berlin 12 August 2020
Transparency-Register ID: 20457441380-38

Preliminary remarks

The German Association of Energy and Water Industries (Bundesverband der Energie- und Wasserwirtschaft - BDEW) represents operators of essential services in the sectors energy and water / wastewater as defined in point (4) of Article 4 of Directive (EU) 2016/1148 (NIS-Directive). The 1,900 companies represented by BDEW differ widely in terms of their size and forms of organisation. The spectrum of the association's members ranges from local and municipal utilities to regional and inter-regional suppliers. They represent around 90 percent of the electricity production, over 90 of electricity grids, over 60 percent of local and district heating supply, 90 percent of natural gas supply as well as 80 percent of drinking water extraction and around one third of wastewater disposal in Germany. This large variety in the German energy and water markets as well as in terms of drinking water supply and wastewater disposal is unique within the European Union.

The availability of essential services is a central requirement for the confidence of citizens in the functioning of their economy, governments and society. Effective protection of essential services can only succeed with a functioning cooperation between public institutions and private or municipal operators of essential services, such as the energy and water industries.

BDEW welcomes the Commission's goal to strengthen cybersecurity of electricity grid operators in Member States and to foster cooperation in this context by means of the present proposal. In the following we refer to the structure of the first Interim Report of 30 April 2020, focusing on the most relevant chapters for the German energy sector. If considered, we believe that these additional remarks on the proposed pillars can support the future drafting process and help achieve a further improvement of cyber resiliency throughout the whole EU.

Content

1 Introduction

The German energy industry holds the view that a Network Code shall be limited exclusively to Transmission System Operators (TSO) and Distribution System Operators (DSO). It is not appropriate to extend the circle of the target audience beyond these as other operators of essential services are not included in the drafting process. However, the report refers multiple times to cyber security aspects beyond the management of electricity grids: “Network Code on cyber security for the electricity sector”, “an issue for the whole Energy chain”, “ the whole electricity value chain” etc. (see pages 1, 6, 7). We advocate for limiting the Network Code to electricity grid aspects. If the intention of the report is to consider other aspects of cyber security, e.g. cyber security of electricity production facilities, but only in the context of grid management, then this should be stated very clearly.

Additionally, the Interim Report refers to “cyber security aspects of cross-border electricity flows”. It should be clarified to what extent this cross-border category will be applied. In other words, whether the code will be applicable only to cross-border electricity flows, or also internal flows that indirectly affect cross-border electricity flows.

1.1 Context

BDEW welcomes the development of an EU Network Code on Cybersecurity to introduce and specify a uniform minimum level of security for electricity grid operators. We are committed to the goal of further increasing the information security of grid operators throughout the EU. To this end, we welcome that a risk-based approach based on international standards such as ISO/IEC 27001 is being proposed. The responsibility to protect grid infrastructures can only be taken by operators of essential services. After all, only operators can implement the technical and organisational measures to strengthen information security in a solution-oriented and efficient way.

1.2 SGTF-EG2 Final Report

No comment

1.3 CEF Report

The referenced CEF Report is not published as of this moment. Nevertheless, the Interim Report draws extensively on the CEF Report’s recommendations in chapters 4.2 and 4.3. Due to this fact, it is impossible to provide substantial comments on these chapters. For the sake of transparency, there is no other way than to reflect this in our rating of these chapters. We recommend publishing the CEF Report as soon as possible and make it available for stakeholders as part of the consultation process.

2 Executive Summary

See more detailed remarks in chapter 4.

3 Timeline

No comment

4 Essential pillars of the Network Code

4.1 ISO/IEC 27001 Certification

BDEW Rating: *3 Recommendation is generally acceptable*

Comment: In European comparison, the requirements for German grid operators are significantly higher than in other EU countries (both in terms of the scope of the companies obliged to implement the measures and the scope of the required measures). For the security of the European interconnected grid, a uniform implementation of measures throughout the Union as well as the comparability of the scope must be ensured: Only in this way a minimum level of security can be ensured in all EU countries.

The recommendation for implementation of ISO/IEC 27001 certification should be based on ISO/IEC 27001 in conjunction with the controls and implementation guidance of ISO/IEC 27019. ISO/IEC 27019 is the sector-specific standard in the ISO/IEC 27K series. It contains both additional implementation guidance to ISO/IEC 27002 as well as additional energy sector specific controls which are not contained in ISO/IEC 27001 Annex A. We therefore advocate incorporating ISO/IEC 27019 as well as pillar 5 Legacy System Protection into pillar 1.

The German energy industry points out that the Network Code's focus on certification may lead to the risk of neglecting the implementation of more practical security measures in OT systems. Mandatory certification may also lead to the false conclusion that if there are commonly agreed scoping principles (which will be hard to achieve) the same minimum level of cyber security will be established. If present national frameworks for certification already achieve the Network Code's security level, they should remain in force.

The transfer of the Network Code requirements for TSOs and DSOs to the provision of generation services (possibly for the general feed-in of electricity) should be excluded as a matter of principle as other operators of essential services are not consulted in the drafting process. Furthermore, cross-border and cross-organisational aspects are mostly of no concern for other operators of electricity generation as they usually cannot be held liable in this regard.

Based on the present Interim Report we observe the following:

Process for identifying “critical” business processes

The Interim Report does not specify who is responsible for the identification of "critical" business processes. Regarding the editorial focus on grid aspects, it could be assumed that this obligation would be destined for grid operators. It should be specified to what extent grid operators are liable for incidents. Incidents might occur at different levels of the supply chain. Grid operators should not be responsible, by default, for incidents that take place outside of their infrastructures.

Identification of cross-border aspects

Concerning the identification of cross-border and cross-organisational risks, the requirements towards companies whose operations do not concern cross-border flows remain unclear. It should be clearly stated that, in those cases, no additional requirements will be put in place for such companies because they operated in “island” mode without affecting the overall electricity supply in Europe. Therefore, the definition of cross-border and cross-organisational effects needs to be clarified before taking any regulatory action.

The proposed approach is of vital importance from the perspective of TSOs facilitating cross-border electricity flows. However, the effort involved in such a risk assessment and treatment seems disproportionate for locally operating DSOs and represents a considerable extension of the scope of responsibility contrary to operational practice and those DSOs' sphere of influence. It seems necessary to either specify and limit this approach more clearly for DSOs or to drop it for locally operating DSOs. The terms "cross-border" and "cross-organisational" should be defined and delimited in the Network Code.

Certification of small DSOs:

The implementation of the NIS directive is differing between Member States. Using the OES concept means that in some management systems very small DSOs will have to be certified which imposes a very heavy burden. According to German regulation, all DSOs are obliged to implement ISO/IEC 27001 and provide extensive certification evidence and documentation to establish and uphold sophisticated information security practices and measures that can be inspected by regulatory authorities.

Applicability of the Network Code in case of no interconnection with other operators

Operators which can prove that no systemic interconnection exists between their OT infrastructure and other operators' OT infrastructure should be exempt from applying the Network Code.

Strict criteria of risk acceptance

The criteria which risks can be accepted, and which cannot, should especially apply to risks with impact to the security of cross-border and cross-organisational electricity supply.

4.2 Common Functional Security Requirements

BDEW Rating: *2 Recommendation is partially acceptable, but lacks legitimacy*

Comment: This recommendation is, in principle, only partially acceptable. It draws to a large extent on a CEF Report which has not been published yet. It is therefore impossible to provide substantial comments.

In European comparison, the requirements for German grid operators are significantly higher than in other EU countries (both in terms of the scope of the companies obliged to implement the measures and the scope of the required measures). For the security of the European interconnected grid, a Europe-wide harmonised implementation of measures is generally recommended, for which the scope must also be comparable between the member states. However, country-specific requirements must be assessed in accordance with the subsidiarity principle. This is the only way to ensure a minimum level of security in all EU countries.

Based on the present Interim Report we observe the following:

Classification Scheme of protection levels

In principle, a common set of functional security requirements based on the business process criticality could be positive. However, on the one hand, established national regulations should be considered since, for example, the German IT security catalogue specifies three security levels (the default protection level is "high"). On the other hand, certain leeway should be given to apply a tailor-made classification scheme of protection levels that reflect the specific operator's environment. Some companies already have well-established graduation levels in place that are more granular. A possible compromise would be to indicate that there should be a minimum of three protection levels, while several gradations are possible.

Furthermore, additional security objectives shall be considered, such as traceability or authenticity. For OT systems it is also usually of more value to talk about criticality of a function than to use the information centric CIA-triangle. Harmonisation of the classification levels throughout the EU implies that conformity assessment should be harmonised, too.

A common set of functional security requirements

As stated, in principle, a common set of functional security requirements based upon the business process criticality could be positive. However, the specific set of measures differs between TSOs and DSOs as well as the risks and vulnerabilities for cascading effects. The approach to risk analysis along the entire electricity value chain appears questionable from an operational point of view and would be difficult to implement in practice. While TSOs and DSOs can intervene in some way in the upstream value chain, these interventions are primarily limited to their own company/sector context. To this extent, the Interim Reports seems to reflect the realities of state-owned companies or other – also government-owned – operators. Having in mind their vital role for the functioning of the overall electricity system, private companies are not to be held liable for the functioning of the national or European market. Therefore, the risk assessment regarding cascading effects, considering the whole electricity value chain, should be performed jointly by all market parties involved, as recommended under 4.3 Cyber Risk Assessment. The cyber risk assessment should consider cases, in which the OT infrastructures of operators do not share interrelations with each other. In other words, interlinkages and / or cascading effects between OT infrastructures should not in principle be presumed, since this would lead to overregulation. Contemplating a compromise, grid level (TSO, DSO) specific sets of functional security requirements should be considered depending on the criticality of specific business processes and data exchange.

Recommendations for non-functional security requirements

In addition to ISA/IEC 62443, which is not energy sector-specific and hardly applied by nearly 2000 operators in Germany, energy sector-specific specifications such as the BDEW/OE Whitepaper for “Requirements for Secure Control and Telecommunication Systems” should as well be included in the definition of a common set of functional security requirements, given the fact that it is internationally distributed and acknowledged.

4.3 Cyber Risk Assessment

BDEW Rating: *3 - 4 Recommendation is generally acceptable, but lacks legitimacy*

Comment: The recommendation is – with reservations – generally acceptable. It lacks legitimacy because the present recommendation draws to a large extent on a CEF Report which has not been published yet. Therefore, our comments are subject to change according to the content of the CEF Report.

In general, we welcome the establishment of working groups representing both ENTSO-E and the EU DSO Entity as well as any additional group of operators affected by this regulation. To achieve the aim of performing detailed cross-border and cross-organisational cyber risk assessments, it is vital that these working groups are formally tasked and sufficiently funded. We agree that an overall big picture regarding the risks for the interconnected European grid system is necessary and should enrich individual TSO and DSO risk assessment processes. Facilitating a structured discussion between TSOs and DSOs on a European level is fundamental in this regard.

As stated, a proof of concept of a Risk Impact Matrix will be delivered within the CEF Report. It is important that this does not imply any obligations to use special gradation levels etc. in company risk assessments, since these are already well-established or regulated by national law. In general, the referenced CEF Report was drafted by TSOs only. However, the concerns of numerous DSOs and potential other operators affected by this regulation should not be neglected. In addition, it should be noted that interventions in operational risk management often involve massive interference with entrepreneurial freedom, thus potentially resulting in significant adjustments of national regulatory requirements. The timely involvement of the European supervisory authority ACER (and possibly ENISA regarding "cyber risk materialisation") in these activities therefore appears to be necessary. A corresponding addition to the chapter is recommended.

4.4 Product Assurance Scheme

BDEW Rating: *2 - 3 Recommendation is partially acceptable*

Comment: This section is unclear in several respects. In principle, a scheme for product assurance can be beneficial for strengthening information security in the energy sector, if it is entirely voluntary and without further obligations for operators. In this way, the conformity of products and components with common security requirements could be classified by operators on an indicative basis, theoretically promoting cost-efficiency. As a guideline for identifying requirements on safety properties of products and components and their procurement, the BDEW/OE Whitepaper shall be considered, since it is widely used and acknowledged both nationally and internationally (see link above).

However, it should be considered that the absolute, small number of internationally successful Product Assurance Schemes shows that effects and benefits can only be exploited extensively in very specific environments and to a very limited extent. The test procedures represent a great effort and there is a risk that the available supplier base will be greatly reduced as a result of this effort.

In detail, the Interim Report lacks rules on how this process should be organised. The following points should be clarified:

- It must be clarified, under which conditions and with whom the results will be shared (There is no recognisable approach on cost distribution. A fixed sharing system also has the disadvantage that operators of essential services will pay for tests which are not relevant for them.),
- Another aspect is that innovative OT approaches regarding efficiency in production will be revealed to competitors in early stages,
- It must be made clear that applying tested products does not release operators from implementing further security measures and risk considerations. The testing schemes should be continuously adapted to new threats,
- The link to certification schemes within the Cybersecurity Act is missing in the current high-level considerations about product assurance schemes.

Overall, a range of open questions remain at this stage. The assumed impact appears to be assessed too optimistically. Thus, including a Product Assurance Scheme in the Network Code at this stage seems to be premature.

Excursus on mandatory product certification in the energy sector

An obligation to certify products and components in the energy industrial environment is a highly sensitive matter and should not be considered lightly. The effects are manifold and difficult to measure in the prevailing complex environment. The German energy industry also points out that a sole obligation to certify individual products and components does not increase the level of protection of an installation. Plant safety is defined by the weakest link in the chain and must always be assessed in the respective context. A high level of protection can only be achieved through the interaction of all components, plant parts and resources (personnel, infrastructure, processes and their regular maintenance and interaction). The existing, risk-based regulatory approach of ISO/IEC 27001 meets this requirement. Furthermore, mandatory certification would limit the variety of products and components available on the market to a few suppliers. It can therefore be assumed that compulsory certification would result in rising prices for products and components, which in turn would influence market prices for the supply of energy throughout the EU.

4.5 Sharing of technical Information

BDEW Rating: *4 – 5 Recommendation is mostly to completely acceptable*

Comment: BDEW welcomes the proposed recommendation as it can provide significant added value in strengthening information security within the European electricity market. Trans-European cooperation on cyber-attacks required by the NIS Directive is currently very limited. Nevertheless, it must be ensured that due to this recommendation no additional expenditures are imposed on operators. Established reporting channels, structures, and processes to National Competent Authorities / National Regulatory Authorities should be built upon to intensify the sharing of technical information at European level. In Germany, the Federal Agency for Information Security (BSI) should therefore assess received incident reports regarding their European relevance and forward them centrally to the respective National Competent Authorities / National Regulatory Authorities of other Member States. Reports should primarily aim to support and protect the European energy market and European companies. An exchange with institutions on other continents should play at most a secondary role. The Network Code should also clarify the process of information sharing from a funding and organisational perspective.

In addition to technical information, an exchange of indicators of compromise and best practices offers high value for operational information security. Also, information about the country where the attack took place and attribution information are of high interest to operators in order to execute their own risk assessment.

4.6 Legacy systems protection

BDEW Rating: *4 – 5 Recommendation is mostly to completely acceptable*

Comment: We fully agree that legacy systems continue to be fundamental to operating grid infrastructure within the EU. Due to the outstanding lifespan of components, security measures are often very diverse in this regard and are hardly applied consistently in the European Member States. The protection of legacy systems is an inherent part of the German IT security catalogues, which is why we see no need for action from the national perspective.

In general, we advocate for dissolving and integrating this pillar into pillar 1 ISO/IEC 27001 Certification or pillar 2 Functional Security Requirements. Furthermore, the energy sector-specific ISO/IEC 27019 should urgently be included within the Network Code since, amongst others, it already contains proven additional measures and information on implementation guidelines on the protection of legacy systems (see ISO/IEC 27019:2017, Control "12.8.1 ENR – Treatment of legacy systems"). The German energy industry considers this to be more appropriate than initiating a separate initiative for the preparation of measures for the protection of legacy systems, as this would only increase the effort involved in ISO/IEC 27001 certification (see chapter 4.1).

5 Champions

We welcome the designation of thematic champions, offering concrete contact persons to resolve comments bilaterally. For the sake of transparency, the sending organisations behind each champion should be indicated.

6 Possible Risks & Obstacles

No comment

7 Conclusion

No comment

Further information

Yassin Bendjebbour
Phone: +49 30 300199 - 1526
yassin.bendjebbour@bdew.de

Johannes Imminger
Phone: +32 277 451 14
johannes.imminger@bdew.de