A cybersecurity framework fit for wind energy

DECEMBER 2021

windeurope.org

WindEurope

EXECUTIVE SUMMARY

The digitalisation and interconnectivity of energy assets have undeniable benefits and are major drivers towards decarbonisation. But they also multiply the risk of cyber-attacks which can impact several interconnected assets simultaneously and can have important socio-economic consequences. Notwithstanding the similarities with other generation assets, there are cybersecurity needs that remain specific to Distributed Renewable Energy (DER) assets. Among these we can highlight three:

- the need for secure remote operation of several geographically separated assets;
- the need for universal definitions and data standards that asset operators can use as a common vocabulary to build universal risk management processes; and
- the need to use common international security standards given the current diversity of options

The revision of the Network Information Security (NIS) Directive, expected by the end of 2021, and the Network Code for Cybersecurity (NCCS), foreseen to be in force by the end of 2023, are excellent opportunities to address these needs. They can reinforce the use of best-suited security standards per technology type and complement these with lacking universal definitions and data standards.

The draft NIS2 Directive currently discussed by the EU institutions lists DER operators as *essential entities* and as such they will have to comply with the respective security rules for medium-sized and large entities. The draft NCCS currently under public consultation suggests a classification of *critical*- and *high*-impact entities and a future Working Group for defining their respective risk management obligations.

It will be crucial that any upcoming specification of requirements for DER considers this fact: **their cybersecurity needs have very little to do with the size of their owning or operating entity** compared to other sectors where IT security is the major concern. **For operators of DER (producers, suppliers, or market participants):**

1) **the legislation should define different types of entities primarily in function of the assets they operate - notably the impact of these assets on cyber resilience - and secondarily in function of their size as entities.** The entity size should only be considered to address an increased IT risk but should not be the main driver
2) **obligations for risk management measures should be set at asset level and attributed to each entity type based on proportionality criteria mainly driven by the level of risk and impact of possible events per type of asset and asset fleet**
3) **the upcoming regulation should incorporate major elements from currently used international standards** that have been developed and applied by the industry at global level since several years
4) **product certification should not be mandatory**. Instead, legislation should set performance-based targets and allow the concerned entities to choose the standard that best suits their security needs and regulated targets. Mandatory product certification could lead to significant costs, hinder innovation and hamper the ability to respond to cyber threats.

1 Cybersecurity in the European electricity sector

The digitalisation and interconnectivity of energy assets have undeniable benefits and are major drivers towards decarbonisation. But they also multiply the risk of cyber-attacks which can impact several interconnected assets simultaneously.

Cyber-attacks can cause physical equipment damage (with potential cascading failures in other interconnected assets), environmental damage, widespread electricity supply disruption with devastating impacts on critical services, households and businesses but also brand image damage of businesses.

Total costs for the asset owner in mitigating these impacts, revenue losses and dealing with the cyber-attack (e.g., investigation, containment…) can run into millions or even billions of euros[1]. Cyber incidents are expected to grow not only in scale but also in cost. The grid has proven its resilience during the Covid-19 pandemic. But the energy system, while undergoing its transformation, needs to be able to withstand a growing number of unforeseen events.

Regardless of any mandatory or prescriptive measures, full protection against cyber-attacks in the electricity sector is impossible. Policy makers should design a wide range of strategies to build up cyber-resilience from prescriptive to performance-based ones. Over-prescriptive policies might allow for a more efficient monitoring of compliance, but they come at a very high cost and they will never be able to cover all potential risks.

The process of improving cyber-resilience should be continuous considering the actual cyber-risk landscape. Setting achievable metrics and targets and giving asset owners room to implement the measures they need to meet these targets can help to build resilience against evolving needs. 2021 will be a reference year for EU legislation in electricity cybersecurity. Two legislative files will be setting new cybersecurity requirements for grid and generation assets at European level:

1. The revised Network Information Security Directive (NIS2 Directive)

The revision of the NIS Directive (NIS2 Directive) is expected to conclude by the end of 2021. Based on the draft proposal by the European Commission (EC)[2] and its suggested amendments by the

[1] International Energy Agency, Power systems in transition, 2020

[2] European Commission, Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020) 823 final), December 2020

European Parliament (EP)[3] and the European Council (EC)[4], the NIS2 Directive will be listing as *essential entities* a large share of generation assets and electricity market participants as well as digitalisation infrastructure providers (e.g. data centre service providers). *Essential entities* will have reinforced cybersecurity obligations.

According to the same proposal, manufacturers of electrical equipment will also be listed as *important entities* with increased security obligations. Wind turbine and component suppliers will also be indirectly impacted by reinforced obligations as suppliers of equipment for *essential entities*.

2. The Network Code for Cybersecurity (NCCS)

The NCCS should provide technical specifications for the compliance of grid, demand, and generation assets with the obligations of the NIS2 Directive. Following the EC's formal mandate[5], ENTSO-E and the EU.DSO entity coordinated the group of entities that developed a draft proposal for the legal text of the NCCS[6,7]. This draft has been under public consultation since mid-November. The final proposal integrating the feedback by stakeholders is foreseen to be submitted to ACER by mid-January 2022. ACER will review and submit the final version to the EC for approval and adoption in 2022. The NCCS should enter into force 18 months after its approval by the EC, most probably by the end of 2023.

Our recommendation is that both legislative items (the NIS2 Directive and the NCCS) consider this crucial aspect: cybersecurity rules for electricity assets must focus on the domain of vulnerabilities of the Operational Technology (OT). We highlight this need because it does not apply for many other sectors - addressed by the NIS Directive - for which the vulnerability of the Information Technology (IT) remains the main concern. Indeed, the development of the NCCS was aimed at addressing such specific needs but the published draft proposal does not address them sufficiently at this stage.

Based on this principle and considering the current policy developments, this paper highlights specific security needs that should be shaping upcoming security rules for wind farm owners as well as for wind

---

[3] European Parliament, Report on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, November 2021

[4] The Council of the European Union, Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148, November 2021

[5] European Commission: Invitation to draft framework guideline on sector-specific rules for cybersecurity aspect of cross-border electricity flows, Reference ARES (2021)653629, January 2021

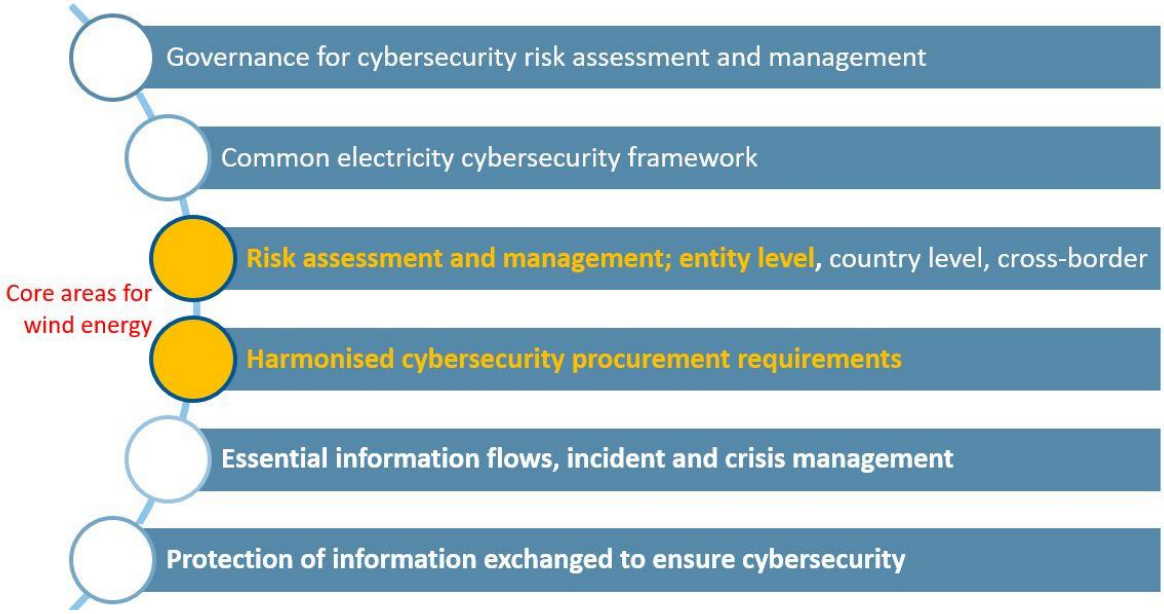
[6] The drafting team of the NCCS is chaired by ENTSO-E and vice-chaired by the EU DSO entity, and it includes the European Commission, ENISA, CEER, ACER, All NEMO Committee, the Regional Coordination Centres (RCCs) and the NIS Cooperation Group.

[7] ENTSO-E, EU DSO entity, Legal text for public consultation: Network Code for cybersecurity aspects of cross-border electricity flows, October 2021

turbine and component manufacturers. It also suggests best practices and existing international standards to be considered in the design of such requirements.

Figure 1 outlines the major areas of the proposed draft NCCS currently under public consultation. Regarding the suggested draft NCCS, the paper presents the wind industry perspective and respective recommendations about the two areas that have been highlighted in **Figure 1**: risk assessment and management at entity level and harmonised cybersecurity procurement requirements.

Figure 1 Major areas in the currently presented draft Network Code for Cybersecurity (NCCS)[7]



2 A cybersecurity framework fit for wind energy

Notwithstanding the similarities with other generation assets and the numerous existing guidelines on the security of Operational Technologies (OT), there are challenges that remain specific to Distributed Renewable Energy (DER) assets. Unlike conventional onsite operations, there is an increasing trend for fully remote operation of DER assets. This requires a much more thorough engineering design to ensure system reliability and safety at acceptable costs. Such design should consider the following needs:

- **Secure remote operation of several geographically separated assets**: most DER will be far away from their actual operations' team and their operation will be mostly handled online. In addition, wind and solar are fully weather dependent. This means that the real-time communication of information on weather, grid capacity and other parameters is extremely valuable and will be increasing the need for larger volumes of data to be transmitted among several parties. As a result, communication channels will multiply and diversify and this will increase the cyber-risk

significantly. One-size solutions and requirements will certainly not fit all needs for security of supply.

- **Need for universal definitions and data standards** that the operators of the various interconnected assets (grid elements, demand, storage, and generation) can use as a common vocabulary to build joint management processes against cyber risk.

  Unfortunately, such a universal "digital vocabulary" that could enable an efficient exchange of real-time information across organisational and geographic boundaries is lacking today. Necessarily this creates a lack of context for setting cybersecurity requirements that are cater to both the existing and emerging decentralised model of power systems.

  Regarding information exchange, the EU Network Code on System Operation (System Operation Guideline)[8] regulates the Key Organisational Requirements, Roles and Responsibilities of grid users and System Operators for the exchange of operation data (known as the KORRR approach)[9]. However, the current lack of harmonisation in the implementation of the KORRR approach leaves space for many different interpretations and flexibility for customisation at national level[10]. As a result, there is no EU-wide model to describe the individual responsibilities of each agent in terms of communication and security, the interactions between the agents and the supervisory flow of control.

  Using different data standards and applying different processes for data exchange among the various systems will not help the implementation of a resilient cross-border cybersecurity strategy. The development of the upcoming NCCS is an excellent opportunity to address this gap in alignment with the EC action plan for the digitalisation of the energy sector[11].

- **Need to use common international security standards:** there are several existing standards for security (e.g. IEC62443, NIST-CSF, ISO27001, JEAG 1111-2019…) and challenges in adopting them uniformly across the DER sector. The main reason is the lack of harmonisation among these various standards. Some of them are specific to DER technologies while others can be applied to a larger variety of technologies.

---

[8] The European Commission, Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation

[9] ENTSO-E, All TSOs' proposal for the Key Organisational Requirements, Roles and Responsibilities (KORRR) relating to Data Exchange in accordance with Article 40(6) of Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a Guideline on Electricity Transmission System Operation

[10] WindEurope, Making wind farms and the power system more interoperable: Focus on data exchange, March 2021

[11] WindEurope, WindEurope response the EU suggested action plan for digitalising the energy sector, September 2021

The current regulatory developments are an excellent opportunity to incorporate the best elements of these standards by technology type into the EU legislation. Creating new requirements that may even conflict with the currently used standards should be avoided to keep the costs of technology down. The role of the NCCS should exactly be to cover any gaps created by the lack of common definitions, data standards and interoperability models.

Clearly the development of any security requirements made for the energy sector requires first a common understanding of IT and OT cybersecurity needs of all types of assets. Today this common understanding does not seem to be sufficiently mature. This was not in the scope of the NIS Directive but must now be addressed in the development of the NCCS.

The proposed draft NCCS suggests the creation of a Working Group that will take forward the detailed technical specification of requirements. Considering the expected volumes of DER in the next decades, this Working Group should directly involve representatives of DER operators and technology vendors for such assets to make sure that all crucial aspects will be adequately evaluated.

2.1 Risk management

Risk assessment strategies should be setting requirements to asset owners in function of the potential impact that compromising each type of their assets would have on the rest of the energy system and on the asset owner itself.

Based on the suggested revision of the NIS Directive currently discussed by the EU Institutions, DER operators are listed as *essential entities.* As such they will have to comply with the respective security rules put forward for medium-sized and large entities. With a similar approach, the draft proposal for the NCCS suggests a classification of *critical*- and *high-impact* entities and a future process for defining their respective cyber-risk management obligations.

As explained in the previous paragraphs**, cybersecurity needs of DER have very little to do with the size of their owning entity (whether it is an SME or a large organisation) compared to other sectors where IT security is the major concern**. In the case of wind farms, the impact of compromising a certain asset or asset fleet is directly linked to the installed power capacity of each specific asset and its interconnections to other grid or generation assets. Security rules, both in the upcoming NCCS and in the revised NIS Directive, need to be designed at asset level considering this crucial fact. In particular:

- **For operators of DER (producers, suppliers, or market participants):**

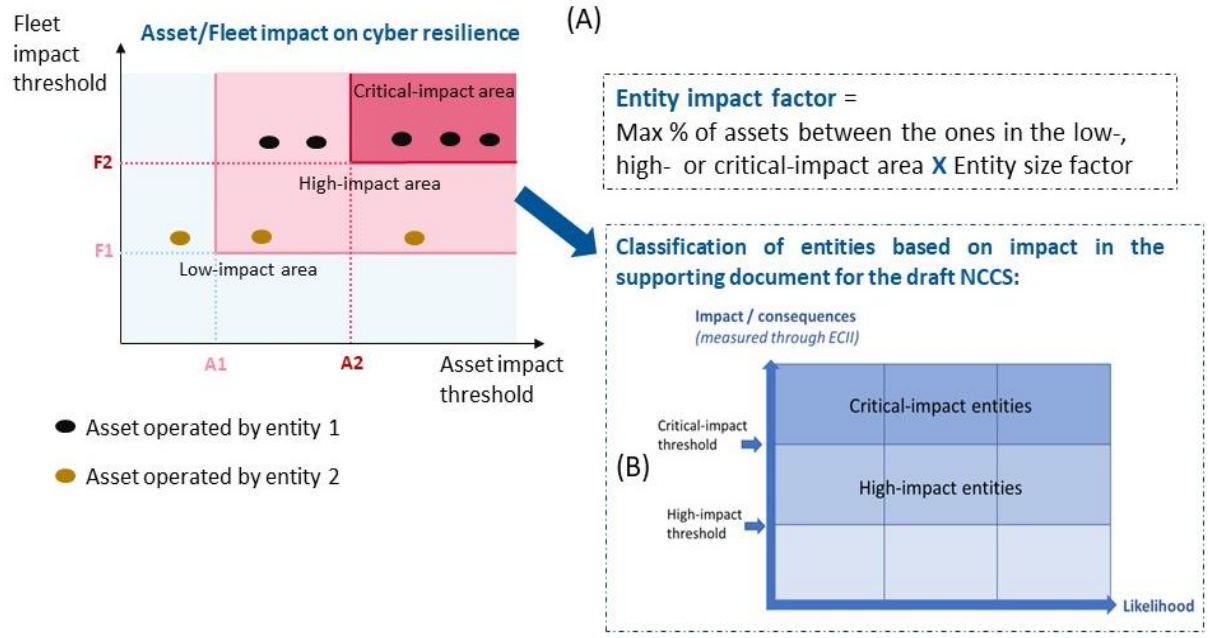
Regulation should define different types of entities primarily in function of the assets they operate - notably the impact of these assets on cyber resilience - and secondarily in function of their size. The size of the respective entity should be considered to address an increased IT risk but should not be the main driver.

Therefore, obligations for risk management measures should be designed at asset level and attributed to each entity type based on proportionality criteria that consider the level of risk and impact of possible events per type of asset and asset fleet.

The legislation should also define different types of assets with thresholds set in function of the installed capacity of the asset (and if necessary additional criteria per case) and of the total capacity of the fleet of assets operated by the same entity (to address the interconnectivity of assets). **Figure 2(A)** presents an illustrative process for classifying assets in a low-impact, high-impact or critical-impact area.

As shown in **Figure 2(A)**, our suggestion is that an *Entity impact factor (*E_{IF}) is attributed to each entity primarily as a function of its share of assets (operated within the same Member State) falling inside the low-, high- or critical impact area, and secondarily of its size as an entity. An *Entity size factor* (E_{SF}) should only be introduced to factor a higher IT risk due to the size of the entity uncoupled with the total power capacity of the fleet that it operates. This factor should not be significantly increasing the *Entity impact factor* for the reasons explained before. The *Entity impact factor* could be used to classify the entities as *high-* or *critical-impact* ones (as currently suggested in the draft NCCS, **Figure 2(B)**).

Figure 2 Illustrative methodology for classifying *critical- and high-impact* assets and entities. Source: (A) WindEurope and (B) ENTSO-E & EU DSO entity



In the chart of **Figure 2(A)** the y-axis represents the total installed capacity of the fleet of assets operated by an entity within the same Member State. The thresholds F1 and F1 could be applied to define whether the total fleet of assets (connected to the grid) of a certain entity should be classified in the low-, high- or critical-impact area in function of the entity's total installed capacity. The x-axis represents the installed capacity of each asset operated by an entity within the same Member State. The thresholds A1 and A1 could be applied to define whether each asset should be classified in the low-, high- or critical-impact area in function of its installed capacity.

Therefore, if an entity operates a total number *S* of assets in a Member State, with *X*% of this *S* falling in the critical-impact area (**Figure 2(A)**), *Y*% falling in the high-impact area and *Z*% falling in the low-impact area (X+Y+Z=100%) then its *entity impact factor* (E_{IF}) should be defined like this:

$$E_{IF} = \max\{0.01 \times (X, Y, Z)\} \times E_{SF} \text{ , with } E_{IF} \leq 1$$

The range E_{SF} should be defined with the Working Group to be formed for the implementation of the NCCS but our initial recommendation is that its value should low (for instance between 1 and 1.1).

With this approach obligations should differentiate at two levels:

- at asset level based on whether an asset is in the low-, high-impact or the critical-impact area
- at entity level based on whether the operating entity is a low-impact, high-impact or critical-impact one for the respective Member State

Critical-impact entities should not have the same obligations for all their assets irrespectively of the impact of these assets. The same should apply for low- and high-impact entities. Also, assets in the critical-impact area should comply to similar obligations which may only slightly differ due to the size of their owning entity.

Creating a competitive advantage for certain sizes of entities would not increase the cyber resilience. This would just lead to the creation of several business structures of a favourable size operating single or limited number of assets but all belonging to the same owner. Therefore, the current entity-size driven perspective in the NIS2 Directive and the draft NCCS is inadequate to cover the cybersecurity needs of DER assets.

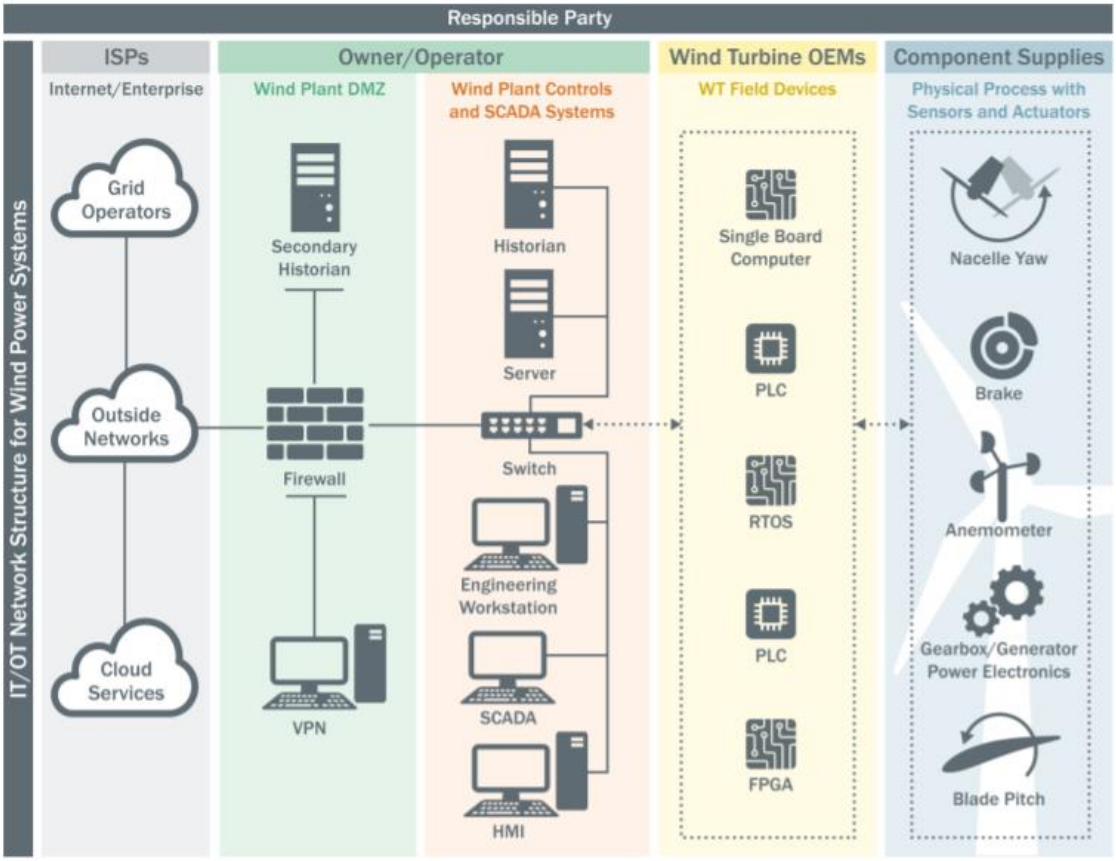
Asset operators are not the only wind sector entities responsible for complying with security rules. Technology vendors are also responsible for ensuring compliance with technical specifications and should be involved in relevant stakeholder processes irrespectively of whether they are listed as *essential* or *important entities* in the updated NIS Directive. **Figure 3** illustrates the IT/OT infrastructure in a wind farm and the respective parties that are responsible for security compliance in the current US framework.

In many cases a single party may perform multiple roles, for example the technology vendor may also operate and monitor the turbines under a contract with the owners. In such cases the responsibility to comply with regulatory requirements should lie both with the asset owner and the technology vendor during the contracted period. A common framework on the expected cybersecurity controls under contractual obligations will greatly benefit the industry by harmonising requirements across the different parties.

➢ For technology vendors of DER equipment:

A similar grading should be created as for DER owners and operators, considering products with different security levels integrated by design. The respective thresholds for equipment, assets and entities should be defined through a formalised process at the EU level involving all relevant stakeholders (e.g., Working Group of the NCCS). They should also be harmonised across Europe to ensure the application of the single EU market concept.

Figure 3 Schematic representation of the IT/OT infrastructure in a wind plant and responsible parties for security. Source: U.S. Department of Energy[12]



2.2 CERTIFICATION

Since several years wind farm operators and technology suppliers have been involved in security standardisation processes together with other relevant stakeholders. The outcomes and ongoing work of these processes should be integrated in the ongoing regulatory developments to ensure that all important aspects have been considered.

To keep technology costs down, we should avoid creating new security rules that do not consider the standards that have been used by the industry at global level since several years. The currently used international standards should be recommended at EU and national level to support the implementation of an actionable risk mitigation strategy.

Specifically, the updated NIS Directive should recommend using the ISO27001 standard or equivalent to be applied by the concerned entities. However, DER owners anand technology suppliers should have the

[12] U.S. Department of Energy, Roadmap for wind cybersecurity, July 2020

option to choose whether they will apply ISO27001 or an equivalent standard regarding the security management process.

When it comes to industrial control cybersecurity applied to wind and solar generation assets, the IEC62443 standard should be the recommended one because it covers the principal functionalities and requirements in a holistic manner. Further to these recommendations, the EC could support the European Union Agency for Cybersecurity (ENISA) to develop an EU minimum applicable standard that could be used by all concerned entities.

However, product certification should not be mandatory. Instead, the legislation should set performance-based targets and the concerned entities should be able to make their choice of standard that best suits these security needs and these regulated targets. Mandatory product certification could lead to significant costs of adoption, hinder innovation and hamper the ability to respond to cyber threats.

Recommendations

This paper presented specific security needs that should be shaping upcoming security rules for wind farm owners and operators as well as for wind turbine and component manufacturers. Below is a list of our recommendations:

- **Governance and engagement of stakeholders**: The proposed draft Network Code for Cybersecurity suggests the creation of a Working Group that will take forward the detailed technical specification of requirements. Considering the expected volumes of DER in the next decades, this Working Group should directly involve representatives of DER operators and technology vendors for such assets to make sure that all crucial aspects will be adequately evaluated.
- **Design of rules and obligations**: The ongoing revision of the NIS Directive and the upcoming Network Code for cybersecurity are excellent opportunities to reinforce the use of best-suited security standards per technology type and to complement these with the necessary universal definitions and data standards. To keep technology costs down, we should avoid creating new security rules that do not consider the standards that have been used by the industry at global level since several years.
- **Obligations for owners and operators of DER**: cybersecurity needs of DER have very little to do with the size of their owning entity (whether it is an SME or a large organisation) compared to other sectors where IT security is the major concern. Therefore, **the legislation should define different types of entities primarily in function of the assets they operate -notably the impact of these assets on cyber resilience - and secondarily in function of their size**. The size of the respective entity should only be considered to address an increased IT risk but should not be the main driver.

  Therefore, **obligations for risk management measures should be designed at asset level and attributed to each entity type based on proportionality criteria that consider the level of risk and impact of possible events per type of asset and asset fleet.**
- **Standards for variable renewables**: the outcomes and ongoing work of international standardisation processes should be integrated in the ongoing regulatory developments to ensure that all important

aspects have been considered. Specifically, the updated NIS Directive should recommend using the ISO27001 standard or equivalent to be chosen by the concerned entities. When it comes to industrial control cybersecurity applied to wind and solar generation assets, the IEC62443 standard should be the recommended one because it covers the principal functionalities and requirements in a holistic manner.

- **Certification**: product certification should not be mandatory. The previously mentioned standards should only be recommended. Instead, the legislation should set performance-based targets and the concerned entities should be able to make their choice of standard that best suits these security needs and these regulated targets. Mandatory product certification could lead to significant costs of adoption, hinder innovation and hamper the ability to respond to cyber threats.