Architecture program

Responses to the EU questionnaire on certification in the Energy sector

Version 1.0

26 November 2019

Version History

Date	Version	Description
7 November 2019	0.1	First draft answers circulated to ENCS members
26 November 2019	1.0	Final version after ENCS member comments

TLP Green – ENCS Members

The European Network for Cyber Security (ENCS) is a non-profit member organization that brings together critical infrastructure stake 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, component and end-to-end testing, as well as education & training.

EU questionnaire on certification

On 2 December 2019, the EU commission held a meeting to assess the need for cyber-security certification of products, systems and services in the Energy sector under the Cybersecurity Act. In preparation to this meeting, they sent a questionnaire to the participants. This document contains the responses from ENCS to their questions.

Questions and answers

What international/European/national cybersecurity standards for energy are you currently using? Please list the most dominant standards you (and your members) are using?

Our members are mostly using ISO/IEC 27001 for their information security management system. For technical requirements, some use IEC 62443 and others the BDEW whitepaper, but there is no clear consensus. Both documents include requirements for the procurement phase of technical components and systems and to processes relevant to the project’s implementation. Parts of IEC 62351 are used for detailed technical specifications.

Do you think we need any additional certifications for cybersecurity in the energy sector? If yes, on what level (product level, service level, process level, people (knowledge, skills) would certification bring most value?

Additional certifications can be useful for products and services (including supplier development, production and delivery processes), but only if a good scheme can be developed for them. Certification may make it easier for grid operators to procure secure products and services. And by giving suppliers a clear target for security, it could lead to more secure products and services.

But it is not clear yet if and how a good certification scheme can be developed. Existing security certification, notably Common Criteria, do not seem a good match for the energy sector. They work best on a small well-define scope, while most grid operators apply a defense-in-depth strategy on a large system level. The IECEE certification based on IEC 62443 is developed for industrial systems and on paper may be a better match. But the IECEE scheme is in our opinion not mature enough to provide strong assurance. We see a risk that because of the European cybersecurity certification framework unproven certification schemes may be rushed into harmonization.

For grid operators, the ISO/IEC 27001 standard and ISO/IEC 27019 with its specialized scope for the energy sector provide a good basis for certifying their critical processes. No additional certification is needed for this.

It is too early to develop schemes for certifying knowledge or skills specifically for the energy sector, as the requirements are evolving too quickly. Training and education are of course very important, and most grid operators are investing heavily in it. General certifications applicable in different sectors can also be useful. But the more specialized, technical roles and responsibilities are not harmonized between grid operators, as they are for more traditional functions. Standard function profiles with required skills and knowledge may crystallize in the future when more grid operators have been using an ISO/IEC 27001 based ISMS for a longer time.

In what areas should new cybersecurity certification schemes be established and at what level (e.g. product, service, process and/or people) should they be harmonised within the EU?

Certification of grid operator critical processes can be established based on the ISO/IEC 27001 standard. Grid operators are familiar with the standard, and it can be adapted well to their situation.

For products, services and skills, a good scheme should first be developed and be used for several years before it would be productive to harmonize it within the EU.

Do you think a network code would be enough to address current gaps related to cybersecurity standards and certification? What would be the best way to ensure compliance?

Larger grid operators are covered by the NIS directive, which already provides a way for regulators to ensure the security of critical infrastructures.

A network code for cyber-security would have the most value if it covers market parties that are not covered by the NIS directive but that are important to grid stability. Examples are smaller grid operators, electric vehicle charge point operators, and operators of distributed energy resources (DER).

Who should check compliance of cybersecurity certified products, services or processes? (E.g. government, energy regulators, third parties, self-assessment, etc.)

Processes and services can be certified by authorized auditors. But some regulatory supervision of the auditors would be desirable to ensure consistent results.

For products, testing by an independent lab is important, as it provides a cost-effective way to assess the security. Self-assessment does not provide enough assurance in most cases.

How could cybersecurity certification bring value to your organisation? What are potential pitfalls for implementing cybersecurity certification?

Certification of grid operator processes allows grid operators to demonstrate to regulators that they are they have functioning security management processes established. It also is a tool for security officers to get sustained commitment to security in their own organization. A high-quality risk management process addressing the right scope is key objective for certification. Certification of a scope not addressing the most critical systems and processes or not providing effective controls would not have the desired effect.

Certification of products and services would bring value by:

- Simplifying procurement. Less time needs to be spent on developing requirements or setting up evaluation against them.
- Giving vendors a clear, harmonized target for security. Vendors can then focus their development efforts on achieving this target, rather than developing custom security features for different TSOs. This should lead to more secure products and services at a reasonable price.

Potential pitfalls for product certification: if quality of requirements to certify against is not good insecure products or services will be certified, taking away incentives for manufacturers and operators to address or improve security. Certification may lead to a false security and maybe mislead the management to not invest in additional security measures or organisations

Moreover, attacker methods and techniques are constantly changing - the certification is only valid for a certain time.

How would you quantify costs and benefits for cybersecurity certification? Would you see a positive business case in additional cybersecurity certification? Please share your reasons.

For processes, our members have the impression that there is a positive business case, but little data is available to substantiate this. Costs for certification and implementation of security organizations are significant but, with an eye on the risks and threads there is also a strong need for it.

Even if the businesscase is not positive, it is an importnat step to develop further

For products and services, the business case would depend on the scheme that would be used. Too strict or unpractical product and process requirements may prohibit adoption by the market (example: German SM certification).

Should cybersecurity certification be mandatory? If yes, how would you determine compliance levels from basic to more advanced at European level, to fit both smaller and bigger organisations?

We think the NIS directive should be leading for grid operator processes. Certification should only be made mandatory if regulators choose this as a way to implement the NIS directive. Making it mandatory through the EU cybersecurity certification framework or a network code if regulators choose other ways to implement the NIS directive would create an extra burden for operators.

We do think a common approach over whole Europe is desirable, as it would make the certifications in the different countries comparable. There is one trans-european grid and bigger incidents in countries would also have effects on other countries and their critical infrastructure

For products, systems, and people, it is much too early to think of making certification mandatory, as no proven schemes are yet available.

How could you tackle supply chain security with cybersecurity certification?

Supply chain security is covered in the ISO/IEC 27001 controls. Certification schemes for products and services should include requirements to suppliers that also improve supply chain security.

Certification should however not be expected to counter advanced (nation state level) threats.

As regards ICT products, how do you capture and express cybersecurity requirements and how do you verify that the requirements are being met by technology suppliers?

ENCS has been supporting its members by developing security requirements sets for procuring OT products. Requirements sets are available for substation automation, distribution automation, smart metering, and electric vehicle charging. The requirements are aligned with the ISO/IEC 27002 and IEC 62443 standards. Many of our members are using the sets in their procurement documents. ENCS is expanding this approach to other grid domains.

ENCS has been supporting members to verify the requirements through its test lab. ENCS provides requirements-based testing for smart meters, data concentrators, RTUs, and EV charging stations.

Do you require (stakeholders) or provide (technology suppliers) cybersecurity certification (independent third party assessment) as evidence of requirement fulfilment?

Many grid operators require suppliers to have an ISO/IEC 27001 certificate when they procure products or services from them. The certification shows that they can properly protect confidential information related to the customer, and so is usually only a part of the requirements sets.

What features of ICT products require particular cybersecurity requirements? Do you require specific requirements for ICT product configuration (e.g. hardening) as well as supplier's development (e.g. secure development) and after-sales processes (e.g. vulnerability disclosure, provision of security updates)?

Requirements for products should cover both the technical security functions on the product and the security processes at the vendor (including development and after sales support). See for examples the requirements sets publicly available through our website (encs.eu).