DSO ENTITY
DSOs FOR EUROPE

European Network of Transmission System Operators for Electricity

entsoe

Supporting document

for the procurement recommendation on substation gateways

1 Introduction

Under Article 35 of the Network Code for Cybersecurity (NCCS), the European Network of Transmission System Operators for Electricity (ENTSO-E) in cooperation with the EU DSO entity (DSO Entity) has developed a proposal for the non-binding cybersecurity procurement recommendations for substation gateways (substation gateway profile). This supporting document has been developed jointly by ENTSO-E and the DSO Entity to accompany these recommendations. It provides all interested parties with information about the rationale for the procurement recommendations for substation gateways.

1.1 Legal status of this document

This document accompanies the non-binding cybersecurity procurement recommendations and is provided for information purposes only. Consequently, this document is not legally binding.

1.2 Work programme

The current profile only covers RTUs and gateways used for substation automation in high-voltage electricity grids. It does not cover other components such as IEDs used within the substation, or RTUs and gateways used in distribution automation for medium-voltage grid.

ENTSO-E and the DSO-entity may develop profiles for such components in the future based on the needs of high- and critical-impact entities. ENTSO-E and the DSO-entity will establish a work programme for such profiles and other recommendations after the regional risk assessment (see Article 35 (1)) of the NCCS).

2 Substation gateway profile

2.1 Substation gateways

The substation gateways are components of automation systems. They are used to remotely monitor and control the electricity grid from the SCADA system located at a control centre. Therefore, this profile concerns mainly TSOs and DSOs, as they are the types of entities, within the NCCS regulation's scope, that use automation systems to control the electricity grid.

2.2 Use of IEC 62443

The substation gateway profile has been developed according to the IEC 62443 standard series (see Figure 1), particularly parts 4-1 and 4-2. IEC 62443-4-1 describes the requirements for secure product development, while IEC 62443-4-2 describes the technical security requirements for components.

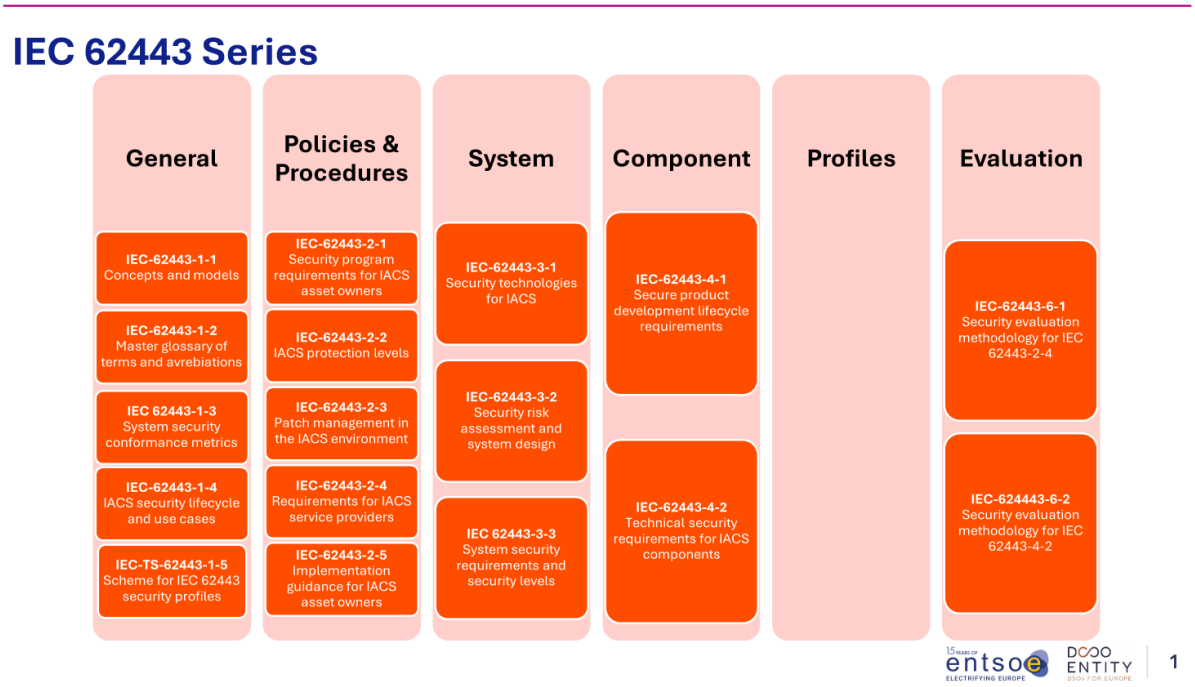

Figure 1 IEC 62443 series

The IEC 62443 standard was selected due to various reasons:

- It is a widely supported standard for industrial cybersecurity, and it counts with support from the industry manufacturers. The SGTF EG2 report [1] states that T&D Europe supports that IEC 62443 is the best option available as it aligns the requirements for systems, products, and service providers.
- It is important to combine technical requirements with secure development when specifying the requirements for devices. IEC 62443 allows to reflect the requirements of the EU Cybersecurity Act by combining the requirements for secure development (IEC 62443-4-1) with technical requirements for devices (IEC 62443-4-2). Moreover, the report on certification published by the Joint Research Centre (JRC) [2] foresees an IEC 62443 certification path using both IEC 62443-4-2 and IEC 62443-4-1.
- IEC 62443-4-1 and IEC 62443-4-2 have been mapped by the JRC and ENISA to the requirements from the Cyber Resilience Act (CRA) and between the two standards they cover most of the CRA requirements [3].

- IEC 62443 has a worldwide supporting ecosystem, comprised of a diversity of certified products, certified professionals capable to perform system integration and testing activities and several accredited third-party testing labs, able to verify or test equipment in conformance to EN IEC 62443.

2.3 Format of the profile

The substation gateway profile follows the *IEC 62443-1-5 - Rules for IEC 62443 profiles*, which defines an IEC 62443 profile as a defined subset of IEC 62443 requirements originating from the IEC 62443 standards which may be adapted to a specific application domain, area of activity or the intended operational environment of a product or automation solution [4]. The structure of this document provides a basis for the later evaluation of the conformance to IEC 62443-4-2 and possible future certification.

The IEC 62443-1-5 rules state that the profile contains a subset of specified IEC 62443-4-2 requirements. The profile must include a justification for the requirements selected; however, the standard does not provide guidance on how to achieve said selection of requirements, it only mentions that the profile should be based on a security risk evaluation when applicable.

The decision for the substation gateway profile was to use a security risk evaluation based on the definition of assets, threats and objectives stemming from the common criteria profiles [5] instead of using security levels that are more common to the IEC 62443. The reason for this decision is to align with the recommendations for cybersecurity certification scheme for industrial control systems from the JRC [2]. The report recommends using a component cybersecurity profile with a component context analysis that includes the description of the intended operational environment, a description of the assets included in the component, a description of the threats applicable to the assets and a description and rationale of the security objectives that will protect against the threats.

The IEC 62443-4-2 requirements are chosen to be those that achieve the objectives defined in line with the ISO/IEC 27002 controls. The objectives are defined to protect against the threats to the assets in scope that have been identified during the threat analysis phase.

2.4 Link to ISO/IEC 27002

ISO/IEC 27002 is a widely used framework for TSOs and DSOs and is one of the standards for controls that are stated in the NCCS' provisional list of European and international standards and controls. In organisations, it is more commonly used than IEC 62443. IEC 62443 is a standard that concerns mainly manufacturers and integrators, since their devices or systems are the ones that should comply with it.

Therefore, it is important to ensure that there is a link between the technical requirements and the information security management systems used by the various entities in scope. This link is achieved through the selection of high-level objectives to protect against the threats identified during the risk assessment. These high-level objectives follow the structure of the controls of the ISO 27002. Then, from the objectives, the required IEC 62443-4-2 technical requirements are selected.

2.5 Contextualizations and interoperability

In the document, the IEC 62443-4-2 requirements may be complemented with a contextualization, interoperability, or implementation guidance. IEC 62443-4-2 requirements are generic allowing for its application in many different domains. The additional information contextualizes the requirements for the scope of substation automation systems.

There are requirements where a contextualization has been added. These contextualizations are part of IEC 62443-1-5 (Contextual mapping) and aim to provide context to the requirement to detail how it must be applied in the context of the substation gateway. The full text of the original requirements as well as the contextualizations must be followed to be compliant with the profile.

Some requirements include additional information for interoperability. In this additional information, a specific technical implementation is recommended to be used with IEC 61850 and IEC 60870-5-104 protocols, following the smart grid sector specific standard series IEC 62351, to achieve cybersecurity interoperability. This additional information is a recommendation and therefore is not mandatory to be compliant with the profile.

An implementation guidance has been included for some requirements to provide additional information and recommendation to profile users. The implementation guidance is not mandatory.

Contextualization	Mandatory for compliance
Interoperability	Optional for compliance
Implementation guidance	Optional for compliance

2.6 Supply chain requirements

According to Article 33(a) of the NCCS, the recommendations for procurement must cover at least:

NCCS requirement	**Covered by substation gateway profile**
(i) the background verification checks of the staff of the supplier involved in the supply chain and dealing with sensitive information or with access to the high-impact or critical-impact assets of the entity. Background verification check may include a verification of the identity and background of staff or contractors of an entity in accordance with national law and procedures and relevant and applicable Union law, including Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and of the Council (18). Background checks shall be proportionate and strictly limited to what is necessary. They shall be carried out for the sole purpose of evaluating a potential security risk to the entity concerned. They need to be proportional to business requirements, the classification of the information to be accessed and the perceived risks, and may be performed by the entity itself, by an external company performing a screening, or through a government clearing;	4.3 – Table 1 - Organizational controls: • 5.20 Addressing information security within supplier agreements
(ii)the processes for secure and controlled design, development and production of ICT products, ICT services and ICT processes,	4.3 – Table 1 - Organizational controls: • 5.21 Managing information security in the ICT supply chain

promoting the design and development of ICT products, ICT services, and ICT processes, which include appropriate technical measures to ensure cybersecurity;	5.1 IEC 62443-4-1 security requirements and maturity level
(iii)design of network and information systems in which devices are not trusted even when they are within a secure perimeter, require verification of all requests they receive and apply the least privilege principle;	4.3 – Table 1 - Organizational controls: • 5.15 Access control • 5.16 Identity management • 5.18 Access rights 5.2.2 FR2: Use control
(iv)the access of the supplier to the assets of the entity;	4.3 – Table 1 - Organizational controls: • 5.20 Addressing information security within supplier agreements
(v)the contractual obligations on the supplier to protect and restrict access to the entity's sensitive information;	4.3 – Table 1 - Organizational controls: • 5.20 Addressing information security within supplier agreements
(vi)the underpinning cybersecurity procurement specifications to subcontractors of the supplier;	4.3 – Table 1 - Organizational controls: • 5.20 Addressing information security within supplier agreements • 5.21 Managing information security in the ICT supply chain
(vii)the traceability of the application of the cybersecurity specifications from the development through production until delivery of ICT products, ICT services or ICT processes;	4.3 – Table 1 - Organizational controls: • 5.21 Managing information security in the ICT supply chain
(viii)the support for security updates throughout the entire lifetime of ICT products, ICT services or ICT processes;	5.1 IEC 62443-4-1 security requirements and maturity level
(ix)the right to audit cybersecurity in the design, development, and production processes of the supplier; and	4.3 – Table 1 - Organizational controls: • 5.20 Addressing information security within supplier agreements
(x)the assessment of the risk profile of the supplier;	Included in Article 3(5) of the methodology.

3 Certification recommendation

The profile does not provide guidance on the use of a European cybersecurity certification scheme as stated in Article 36(1) of the NCCS regulation for two main reasons:

- There is no scheme available yet for IEC 62443 or industrial components. On the Union Rolling Work Programme for European cybersecurity certification [6], ENISA points to areas where European cybersecurity certification schemes might be developed to follow legislation. It includes IACS and IoT products on the section named “Other areas for reflection regarding cybersecurity certification”, which sets them as a possible future scheme to be developed, but not a priority for the coming years.
- There are already generic schemes available for product certification, namely the EUCC [7]. The Common Criteria based on the ISO/IEC 15408 series was deemed as not suitable for IACS components used in the electrical grid by the SGTF EG2 [1] given the complex and varied nature of the energy systems. The Common Criteria entails an in-depth evaluation of the product for the certification that, while beneficial for devices with reduced complexity, might not be feasible or practical for complex systems. Moreover, while the Common Criteria focuses on implementing all security in the product itself, this is not the reality for products placed in energy systems, such as substation automation systems, where also defence-in-depth plays an important role.

A certification scheme for IEC 62443 is available under the IECEE. This scheme however is not a European cybersecurity certification scheme. Hence, we cannot provide a guidance on its use under the NCCS.

4 References

[1] 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,” 2019.

[2] JRC, “Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS),” 2020.

[3] Joint Research Centre & ENISA Joint Analysis, “Cyber Resilience Act Requirements Standards Mapping,” 2024.

[4] IEC, “IEC TS 62443-1-5:2023 Security for industrial automation and control systems - Part 1-5: Scheme for IEC 62443 security profiles”.

[5] ISO/IEC, “ISO/IEC 15408-1:2024 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model”.

[6] European Commission, “ENISA,” 2024. [Online]. Available: https://certification.enisa.europa.eu/about-eu-cyber-certification/eu-regulatory-context/union-rolling-work-programme_en.

[7] ENISA, “Cybersecurity Certification: EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS,” 2021.