



*Establishment of a FramewORk for Transforming current
EPES into a more resilient, reliable and secure system all
over its value chain*

D6.8 Relevant eFORT standardization framework inventory and contributions to existing regulations



Document details

Deliverable no	D6.8
Deliverable name	Relevant eFORT standardization framework inventory and contributions to existing regulations
Version	1.0
Release date	27/08/2026
Type	R (Report)
Dissemination level	PU (Public)
Status	Final
Author	Organisation – Name of writer(s) ENCS – Héloïse Enjalbal, Elvira Sánchez Ortiz, Elisabetta Provvedini, Maarten Hoeve DNV – Klaus Kursawe, Gianni Pagani, Theo Bosma



DISCLAIMER OF WARRANTIES

This document has been prepared by eFORT project partners as an account of work carried out within the framework of the EC-GA contract no. 101075665.

Neither Project Coordinator, nor any signatory party of eFORT Project Consortium Agreement, nor any person acting on behalf of any of them:

- a) makes any warranty or representation whatsoever, expressed or implied,
 - I. with respect to the use of any information, apparatus, method, process, or similar item disclosed in this document, including merchantability and fitness for a particular purpose, or
 - II. that such use does not infringe on or interfere with privately owned rights, including any party's intellectual property, or
 - III. that this document is suitable to any particular user's circumstance; or
- b) assumes responsibility for any damages or other liability whatsoever (including any consequential damages, even if the Project Coordinator or any representative of a signatory party of the eFORT Project Consortium Agreement has been informed of the possibility of such damages) resulting from your selection or use of this document or any information, apparatus, method, process, or similar item disclosed in this document.

This work has been Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor the granting authority can be held responsible for them.



Document history

Version	Date of issue	Content and changes	Edited by
0.1	09/02/2026	First draft Task 6.5	DNV
0.2	26/03/2026	First draft Task 6.6	ENCS
0.3	10/07/2026	Draft deliverable D6.8	DNV, ENCS
0.4	21/07/2026	Deliverable for internal review	DNV, ENCS
0.5	11/08/2026	Peer reviewed	RINA
0.6	21/08/2026	Final review	CIRCE
1.0	27/08/2026	Final report	DNV, ENCS



Table of contents

Executive summary	10
1 Introduction	11
2 Deliverable context and methodology	12
2.1 Outline of the deliverable	13
3 eFORT KERs and demonstrations	14
3.1 Demonstrations within eFORT project	14
3.1.1 Demo 1 – Spain	14
3.1.2 Demo 2 – The Netherlands	15
3.1.3 Demo 3 – Italy	15
3.1.4 Demo 4 – Ukraine	15
3.2 eFORT Key Exploitable Results (KERs)	16
4 Regulations & Standards analysed	18
4.1 Regulations	18
4.1.1 General Data Protection Regulation (GDPR)	18
4.1.2 Artificial Intelligence (AI) Act	18
4.1.3 Cyber Resilience Act (CRA)	19
4.1.4 Network and Information Systems (NIS) 2 Directive	20
4.1.5 Network Code on Cybersecurity (NCCS)	21
4.1.6 Critical Entities Resilience (CER) Directive	22
4.2 Standards	23
5 Gap analysis	24
5.1 Regulations	24
5.1.1 KERs that are compliant with grid security regulations	24
5.1.2 KERs that contribute to the fulfilment of grid security regulations	27
5.2 Standards	35
5.2.1 Security Framework Standards	36
5.2.2 Communication Standards	38
5.2.3 Technical standards	47
5.2.4 Synthesized requirements	50



5.2.5 KERs that support the framework standard IEC 62443	56
6 Recommendations and Conclusions	59
6.1 Regulations & cost-benefit considerations	59
6.2 Standards	60
6.3 Compliance and certification	61
6.4 Training and Information Sharing	62
7 References	63
ANNEX I eFORT Task 6.5 & 6.6 Questionnaire	64
ANNEX II Definition of Key Exploitable Results (KERs)	66
ANNEX III Results survey on EU regulations	68
ANNEX IV Results survey on IEC 62443	107
ANNEX V Relevant OT Communication Protocols	112
ANNEX VI Foundational Requirements (FR1-7)	125



List of figures

Figure 1. Representation of Purdue Model (left) (Kruimer, 10 June 2026) and OSI model (right)	39
---	----

List of Tables

Table 3-1: eFORT KERs relevant to Deliverable 6.8	16
Table 5-1. KERs and their compliance status with grid security regulations	24
Table 5-2. KERs supporting EU regulations	27
Table 5-3. Foundational Requirements FR1-7 - Modbus assessment.....	44
Table 5-4. Foundational Requirements FR1-7 – IEC 61850.....	45
Table 5-5. Foundational Requirements FR1-7 – IEC 62351.....	46
Table 5-6. KERs supporting IEC 62443	56
Table 7-1. KERs supporting IEC 62443- detailed.....	66
Table 7-2. Foundational Requirements FR1-7 - Deterministic Ethernet with MACsec and MKA assessment.....	112
Table 7-3. Foundational Requirements FR1-7 - CANsec assessment.	114
Table 7-4. Foundational Requirements FR1-7 - 450connect assessment.	115
Table 7-5. Foundational Requirements FR1-7 - DNP3 assessment.....	116
Table 7-6. Foundational Requirements FR1-7 - IEC 60870-5-104 assessment.....	117
Table 7-7. Foundational Requirements FR1-7 - CoAP assessment.	118
Table 7-8. Foundational Requirements FR1-7 - DLMS/COSEM assessment.....	119
Table 7-9. Foundational Requirements FR1-7 - M-Bus / Wireless M-Bus assessment.	120
Table 7-10. Foundational Requirements FR1-7 - MQTT assessment	121
Table 7-11. Foundational Requirements FR1-7 - NB-PLC assessment.....	122
Table 7-12. Foundational Requirements FR1-7 - OPC-UA assessment.....	123



Abbreviations and Acronyms

Acronym	Description
AES	Advanced Encryption Standard
AI	Artificial Intelligence
CER	Critical Entities Resilience
CINEA	European Climate, Infrastructure and Environment Executive Agency
CRA	Cyber Resilience Act
CRoF	Control Room of the Future
CSIRT	Computer Security Incident Response Team
CSOC	Cyber Security Operations Centre
DER	Distributed Energy Resources
DNV	Det Norske Veritas
DPIA	Data Protection Impact Assessment
DSO	Distribution System Operator
EC-GA	European Commission Grant Agreement
ECII	European Cybersecurity Impact Index
ENCS	European Network for Cyber Security
EPES	Electric Power and Energy System
EU	European Union
EV	Electric Vehicle
FR	Foundational Requirement
GDPR	General Data Protection Regulation
HV	High Voltage
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology



Acronym	Description
JSC	Joint Stock Company
KER	Key Exploitable Result
LV	Low Voltage
MSSP	Managed Security Service Provider
MV	Medium Voltage
NCCS	Network Code on Cybersecurity
NIS2	Network and Information Systems Directive 2
OPC UA	Open Platform Communications Unified Architecture
OT	Operational Technology
PU	Public
PV	Photovoltaic
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SOC	Security Operations Centre
SOAR	Security Orchestration, Automation and Response
TSO	Transmission System Operator
TU	Technical University



Executive summary

This deliverable reports on eFORT standardization and regulation results from Task 6.5 and Task 6.6. The regulatory framework considered consists of the General Data Protection Regulation (GDPR), the Artificial Intelligence (AI) Act, the Cyber Resilience Act (CRA), the Network and Information Systems (NIS2) Directive, the Network Code on Cybersecurity (NCCS), and the Critical Entities Resilience (CER) Directive. The analysed standards are categorized into framework standards, communication standards and technical standards. IEC 62443 is identified as the most comprehensive cybersecurity framework for industrial and power-system environments and is therefore used as the primary reference framework standard.

The work presented in this deliverable builds on the results and experiences of the four eFORT demonstration sites in Spain, the Netherlands, Italy and Ukraine, together with the developed and tested eFORT Key Exploitable Results (KERs). Through expert analysis and surveys, the practical applicability of cybersecurity standards and the compliance of the eFORT KERs with grid security regulations are analysed. This work also includes the contribution of the eFORT KERs to the fulfilment of regulations and standards requirements.

The results indicate IEC 62443 as the most comprehensive and relevant OT cybersecurity framework for future power systems since it covers both architecture and device security, while also identifying important gaps in current standards related to distributed energy resources, cloud integration, artificial intelligence, quantum-safe cryptography, large-scale key management, and cyber-physical resilience. The project's KERs contribute to key capabilities and requirements from regulations such as risk assessment, security monitoring, incident detection and response, training, resilience testing, and security operations. Overall, eFORT shows that combining technical innovation with standards-based approaches can significantly strengthen the security, resilience, and regulatory readiness of future European electricity networks.



1 Introduction

The power system, as we know it today, is undergoing several parallel shifts at the same time. It shifts from centralized generation (large plants) to a more distributed architecture, with large-scale renewables like offshore wind and utility photovoltaic (PV) and distributed energy resources (DER) like rooftop PV, batteries, local wind farms or electric vehicles (EVs). This results in a decentralized grid, where power flows are less predictable and no longer one-directional. The distributed architecture has one common denominator: a shift towards communicative and software controllable power electronics.

Multiple sectors are being increasingly electrified, shifting energy use from carriers like oil and gas towards the power grid. This shift is reflected in the electrification of transport, domestic and office heating through heat pumps, or industrial electrification.

Besides the growth in volume, the demand grows in complexity. The stronger coupling between power, heat, transport, and hydrogen systems triggers the need for flexibility and capacity expansion. Flexibility is thus shifting from traditional flexibility, through control of dispatchable generation, to distributed and digital flexibility. This flexibility can come from services like short-term balancing, congestion management, arbitrage or behind-the-meter optimization and be provided by DER.

With these parallel shifts in mind, it is no surprise that digitalization becomes the backbone of power system operation. Future grids are fully digital and data-driven systems with real-time monitoring through sensors, smart meters, IoT, cloud-based analytics and control platforms, and AI-based forecasting and optimization. Digitalization enables near real-time system balancing, predictive maintenance and asset optimization and autonomous or semi-autonomous grid operation.

At the same time digitalization also creates strong dependency on communication systems and a tight coupling between cyber and physical domains. Cybersecurity has become a core engineering discipline of the power system, on par with protection, stability, and reliability.

Modern smart grids feature millions of connected endpoints and bidirectional data flows, creating vulnerabilities that could endanger the operation of the electricity grid. Therefore, European cybersecurity regulations and standards are shifting the focus to address the interconnectedness of the grid and to ensure all new parties and technologies are contributing to keeping the grid secure.

Creating regulation and agreeing on standards is a lengthy process and technologies and solutions, both offensive and defensive, develop fast. This report discusses how the outcomes from the eFORT project comply with and support new regulations and standards. Based on the experience from the eFORT project and working experience of the partners, this report presents a standards gap analysis and suggests applicable requirements from existing standards, to provide best practice recommendations to, ultimately, protect the energy grid.

On the regulatory side, European regulations that apply to the eFORT solutions and to the operators who will use them were set out. An analysis of whether Key Exploitable Results (KERs) were compliant with relevant regulatory obligations was conducted. In a second analysis, each KER was assessed against the specific regulatory provisions it can help satisfy. A set of recommendations was developed based on these two analyses.



2 Deliverable context and methodology

In general terms, rules, regulations, directives and legislation formulate the requirements (what needs to be done) and standards support in the actual work (how it can be done). Certification or conformity assessments can provide evidence that specific requirements have been met (the proof). Sometimes regulations refer to standards, sometimes it is left open how to comply to certain regulations. This deliverable focuses on the regulatory and standards framework that underpins compliance. Standards were addressed by Task 6.5 and regulations were addressed by Task 6.6.

At the basis of the regulatory analysis and one part of the standards analysis are the Key Exploitable Results (KERs). KERs are the specific outputs of the project, such as tools, methods, prototypes, datasets, or software solutions, that carry value beyond the project itself. They are developed and validated through the project's demonstrators where they are tested in real operational conditions. Only those KERs applicable to cybersecurity regulations and standards are considered in this Deliverable.

Task 6.5 consists of three parts. The first part evaluates cybersecurity standards and communication protocol challenges in operational environments. To support this analysis, interviews were conducted with representatives from each of the eFORT demonstrations to gather insights on the applicability of standards, implementation challenges, and practical constraints encountered in the field.

The second part assesses how the KERs can support relevant cybersecurity standards, with a particular focus on IEC 62443. The assessment considered where each KER could contribute to compliance with the standard or support its practical implementation in operational technology (OT) environments. The assessment was carried out in two steps. First, an expert assessment was conducted to identify where the KERs support the IEC 62443 framework. Second, the results were validated through a survey of the task leaders responsible for the relevant KERs.

The last part of Task 6.5 focuses on the standards themselves. Its purpose is to identify gaps in both higher-level standards and technical protocols and to develop practical recommendations for a secure power system. As different standards address different aspects of cybersecurity, the gap analysis distinguishes between security framework standards, communication standards, and technical standards.

Task 6.6 focuses on two complementary analyses: the compliance of KERs with grid security regulations and the contribution of KERs to the fulfilment of such regulations. The regulatory framework considered consists of the General Data Protection Regulation (GDPR), the Artificial Intelligence (AI) Act, the Cyber Resilience Act (CRA), the Network and Information Systems (NIS2) Directive, the Network Code on Cybersecurity (NCCS), and the Critical Entities Resilience (CER) Directive. As part of the analysis conducted in Task 6.6, a survey was distributed to the relevant task leaders to identify which KERs are subject to cybersecurity regulations and to gather information on how these regulatory requirements are addressed.



2.1 Outline of the deliverable

Following the introduction and methodology in Sections 1 and 2, Section 3 presents the eFORT demonstrations and the KERs that form the basis of the analysis. Section 4 establishes the assessment framework by describing the regulations and standards considered in the study. Section 5 contains the main analysis, including the assessment of KER compliance with regulations, their contribution to regulatory requirements, the standards gap analysis, and the evaluation of KER support to cybersecurity standards. Finally, Section 6 translates the findings into recommendations and conclusions relating to regulations, standards, compliance and certification, and training and information sharing, while the annexes provide supporting questionnaires, surveys, deep dives into communication protocols and reference material.

To facilitate the reading of this deliverable, readers can distinguish between content related to standards and communication protocols, and content related to regulations. The KERs that form the basis of the regulatory and the relevant standards analyses are described in Section 3.1. The standards analysis, developed under Task 6.5, is presented in Sections 3.1, 4.2 and 5.2. The content related to the regulatory analysis, developed under Task 6.6, is presented in Sections 4.1 and 5.1. Finally, for the recommendations and conclusions of this deliverable, refer directly to Section 6.



3 eFORT KERs and demonstrations

This chapter links cybersecurity regulation and standards with the eFORT demonstrators and introduces the KERs. Section 3.1 describes the four demonstration sites and summarizes the assessment of challenges associated with implementing relevant standards in operational environments. Section 3.2 presents the eFORT KERs, which form the basis for the regulatory and standards analysis discussed in the subsequent chapters.

3.1 Demonstrations within eFORT project

To evaluate cybersecurity standards and communication protocol challenges in a real environment, interviews were conducted with representatives from each of the eFORT demonstrators. Overall, the demos show that formal cybersecurity standards remain relevant as reference frameworks, but their direct implementation is constrained by the specific technical, operational and organisational conditions of each specific environment (see also ANNEX IV for survey results ANNEX I).

3.1.1 Demo 1 – Spain

The demonstration focuses on integrating the DSO's custom systems into micro-grids, using a three-layered approach. First, at the IoT level, a controlled lab environment is used to apply methodologies for mitigating large-scale attacks on distributed energy resources. This includes identifying vulnerabilities, developing preventive action plans, and testing the system's response and resilience through fault simulations. Second, the SecureBox solution is evaluated to assess industrial devices, focusing on status monitoring, security patching, alarms, and emergency functions. Third, operational technologies and strategies from other eFORT work streams are applied to modernize the DSO substation, with particular attention to improving user management, secure access, and activity monitoring.

The main asset involved is the distribution network in Escúzar, operated by the DSO Cuerva Energía S.L., which forms the backbone of the Granada Smart Grid Living Lab. The medium-voltage grid connects directly to the high-voltage network via the Escúzar substation, built in 2008. This network supplies the village of Escúzar and nearby areas, serving residential, commercial, and industrial users. It also integrates significant renewable energy sources, including two photovoltaic plants and multiple residential self-generation systems, contributing to enhanced grid resilience and reliability.

Standards such as IEC 62443 and IEEE references were used as guidance. The inherent complexity of OT environments made it challenging to directly implement them, including the need for stronger motivation and clearer applicability for asset owners, and the relevance of updating standards to address new threats such as AI and quantum safety.



3.1.2 Demo 2 – The Netherlands

Using the Control Room of the Future (CRoF) for TSOs at TU Delft, the demo aims to enhance the resilience of interconnected European power grids against cyberattacks and other hazards. It addresses multiple layers of the system, including infrastructure, hardware, software, and organizational processes. The approach focuses on deploying a real-time digital twin of interconnected grids to assess threats, understand cascading failure effects, and test advanced techniques for strengthening both cyber and physical resilience.

The demo mainly followed literature-based methodologies rather than formal cybersecurity standards such as IEC 62443, IEC 61850, or other established frameworks. Given the specific configuration of the demo setup, applying these standards directly was challenging, as their scope and assumptions did not fully align with the characteristics of the demonstration environment.

3.1.3 Demo 3 – Italy

The objective is to demonstrate grid-islanding algorithms that prevent power outages and ensure quality of the grid service. The approach includes implementing a control scheme for islanded operation to enhance operational resilience, using digital twins of the power system to optimise data exchange, and advancing system digitalisation. Grid observability is improved through the development of a dispatching platform for the DSO control centre, alongside smart procedures for remotely controlling distributed energy resources. A consumer-oriented ChatBot is introduced to support engagement and interaction.

The demo site is the distribution system in the Sarentino Valley in Northern Italy, operated by EDYNA. This network supplies a diverse set of customers, including sub-DSOs. The pilot demonstration is applied in both the medium-voltage (MV) and low-voltage (LV) grid connected to the HV/MV Sarentino substation.

The demo focused on a software platform operating in parallel with the existing EDINA DSO SCADA environment, using an OPC UA interface as the only communication method approved by the DSO. The demo did not follow directly formal cybersecurity standards such as IEC 62443, IEC 61850, or other established frameworks as it was not its primary focus.

3.1.4 Demo 4 – Ukraine

The demo project aims to develop a resilient substation, with a strong focus on substation system security, robust design, and the use of advanced information technologies in both system development and operation. The approach centres around testing project-developed solutions that enhance the security and resilience of substation automation systems. This includes validating technologies in a controlled laboratory environment, selecting the most suitable solutions, and evaluating them using the SecureBox platform. Additionally, the project tests strategies for access control, detection of abnormal behaviour, and the generation and handling of corresponding security alerts.



The demonstration is carried out at a 110/35/10 kV substation in Ukraine. The substation supplies electricity to residential and non-residential consumers.

The Ukraine demo highlighted the operational reality of managing cybersecurity and grid resilience under wartime conditions. The operator is not currently implementing standards such as IEC 62443 or IEC 61850 in live systems, mainly due to regulatory priorities, and the urgent need to restore damaged infrastructure which restricts the budget for the processes required to implement standards across an organization. Cybersecurity is addressed through practical measures such as strict IT/OT separation, isolated OT networks, tunnelling and encryption, backup control rooms, and the ability to operate substations manually. SecureBox is seen as a promising device for improving substation resilience, but the current focus remains on survival, restoration, and knowledge development. The eFORT project is helping build expertise for a future migration from legacy systems to IEC 61850 once infrastructure reconstruction becomes feasible.

3.2 eFORT Key Exploitable Results (KERs)

The KERs are the specific outputs of the project with a lasting value as introduced in Section 2 and are related to the project's demonstrators described in Section 3.1. They are developed and validated through the project's demonstrators, where they are tested under real operational conditions. This provides valuable insights into the challenges associated with the applicability and implementation of regulations and standards in operational environments that are eventually translated into gaps. Table 3-1 presents the KERs relevant to this Deliverable for both Task 6.5 and Task 6.6. Not all project KERs appear, as only those to which cybersecurity regulations and standards apply were selected according of the scope of this Deliverable. For a detailed description refer to ANNEX I/ANNEX II.

Table 3-1. eFORT KERs relevant to Deliverable 6.8

KER	KER Name
1	eFORT Intelligent Platform
2	Data Base Tool
3	Secure Box
4	CRoF training and digital twin environment
6	Dynamic Risk Assessment Tools
7	Islanding Operation Module
8	IDS (Intrusion Detection System)
9	SIEM (Security Information and Event Management)



KER	KER Name
10	Chatbot
11	Guide of recommendations for the safe design of substations
12	RTU (Remote Terminal Unit)
13	Blockchain for grid resiliency
14	SOAR (Security Orchestration, Automation and Response)
15	Blueprint for EPES SOC infrastructure
21	Connected devices vulnerabilities



4 Regulations & Standards analysed

4.1 Regulations

The following section describes the regulations analysed as a part of Task 6.6 covering both the analysis of KERs that are compliant with grid security regulations (Section 5.1.1) and of KERs that contribute to the fulfilment of grid security regulations (Section 5.1.2).

4.1.1 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, lays down rules on the processing of personal data. What triggers it is the processing of personal data, meaning any information relating to an identified or identifiable natural person (Art 4(1)): a name, an identification number, an online identifier such as an IP address, images, sounds, biometric or genetic data. In the solutions developed in the eFORT project that could cover logs, user activity, energy-consumption data and administrator details.

Where no personal data is processed, the GDPR imposes no obligations. Where a KER processes personal data, the baseline obligations apply. They fall on the controller, and in part on the processor (Art 4(7) and 4(8)). Where personal data is processed, the controller must:

- Rely on a lawful basis (Art 6). For security monitoring this is normally the controller's legitimate interests (Art 6(1)(f)); Recital 49 expressly recognises network and information security as such an interest.
- Respect the processing principles of Article 5, including data minimisation, storage limitation, and integrity and confidentiality, and be able to demonstrate compliance (Art 5(2)).
- Ensure security of processing through technical and organisational measures appropriate to the risk, illustrated by pseudonymisation and encryption, ongoing confidentiality, integrity, availability and resilience, restoration after an incident, and regular testing (Art 32).
- Implement data protection by design and by default (Art 25).
- Notify personal data breaches to the supervisory authority within 72 hours where feasible (Art 33), and to affected individuals where the risk is high (Art 34).
- Where relevant, carry out a DPIA for high-risk processing (Art 35), maintain records of processing (Art 30), and conclude a processor contract for outsourced processing (Art 28).

4.1.2 Artificial Intelligence (AI) Act

The Artificial Intelligence Act (Regulation (EU) 2024/1689) establishes harmonised rules on artificial intelligence. It classifies AI by risk: unacceptable risk, high risk, limited risk and minimal risk. AI systems intended to be used as safety components in the



management and operation of critical infrastructure, including the supply of electricity, are classified as high-risk under Annex III, point 2 of the Act.

The cybersecurity obligations for high-risk AI systems apply from 2 August 2026, the general application date set in Article 113, which governs Annex III systems in the Act. These obligations fall on the provider. The provider must:

- Design and develop the system to achieve an appropriate level of cybersecurity, together with accuracy and robustness, and ensure it performs consistently in that respect across its whole lifecycle (Art 15(1)).
- Make the system resilient against attempts by unauthorised third parties to alter its use, outputs or performance by exploiting vulnerabilities (Art 15(5), 1st subpara).
- Keep the technical solutions proportionate, appropriate to the relevant circumstances and the risks (Art 15(5), 2nd subpara).
- Where appropriate, include measures to prevent, detect, respond to, resolve and control AI-specific attacks: data poisoning, model poisoning, adversarial examples or model evasion, confidentiality attacks, and model flaws (Art 15(5), 3rd subpara).
- Declare the level of cybersecurity against which the system was tested and validated in the instructions for use (Art 13(3)(b)(ii)).

Neither limited-risk nor minimal-risk AI carries a mandatory cybersecurity obligation under the AI Act.

4.1.3 Cyber Resilience Act (CRA)

The Cyber Resilience Act (Regulation (EU) 2024/2847) establishes horizontal cybersecurity requirements for products with digital elements. It applies to products made available on the market whose intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network (Art 2(1)). Its obligations fall primarily on the manufacturer, with lighter duties for importers and distributors. From December 11, 2027, manufacturers may only sell products in the EU if they meet these requirements.

The CRA puts essential cybersecurity requirements on all products with digital elements.

Essential cybersecurity requirements (Annex I of the CRA) are divided in two parts:

- Part I, product properties. Products must be placed on the market with no known exploitable vulnerabilities, in a secure-by-default configuration, with protection against unauthorised access, confidentiality and integrity of data, minimised attack surface, and resilience against denial-of-service.
- Part II, manufacturer processes. Vulnerability handling across the support period, a software bill of materials in a machine-readable format, a coordinated vulnerability disclosure policy, and free security updates.

The detailed technical requirements will come from harmonised standards, currently under development. These are split into horizontal standards covering the essential requirements and vertical standards for specific important and critical product categories.



Before placing a product on the market, the manufacturer must show that these requirements have been met. This is done through a conformity assessment. A conformity assessment is the procedure by which compliance with the Annex I of the CRA essential requirements is verified, either by the manufacturer itself or by an independent body, before the product receives its CE marking and can be sold. The CRA sets out several assessment routes, and which one a manufacturer may use depends on the product's category.

Conformity assessment (Article 32), by category:

- **Default products.** Self-assessment under internal control (Module A). Manufacturers may voluntarily choose a stricter route. No independent verification.
- **Important, Class I (Annex III of CRA).** Self-assessment is available only where the manufacturer has applied harmonised standards, common specifications, or a European cybersecurity certification scheme; otherwise, third-party assessment by a notified body is required (Art 32(2)).
- **Important, Class II (Annex III of CRA).** Third-party assessment is mandatory (Art 32(3)), via EU-type examination plus conformity to type (Modules B and C), full quality assurance (Module H), or a European cybersecurity certificate at assurance level at least "substantial".
- **Critical (Annex IV of CRA).** Normally treated the same as important class II products. However, the Commission can make it mandatory through a so-called delegated act, that the products undergo certification. The certification would be done through a European cybersecurity certification scheme.

Classification depends on the product's core functionality.

4.1.4 Network and Information Systems (NIS) 2 Directive

The NIS2 Directive (Directive (EU) 2022/2555), published in December 2022 and currently being transposed into national law by Member States, aims to strengthen cybersecurity across the EU by introducing more stringent requirements for a broader range of sectors. It applies to public or private entities of a type listed in Annex I or Annex II of the Directive that qualify as medium-sized enterprises, or exceed those ceilings, and that provide their services or carry out their activities in the Union (Art 2(1)). The obligations of NIS 2 fall on the entity.

The entity must:

- Ensure its management body approves the cybersecurity risk-management measures and oversees their implementation and can be held liable for failures; members must follow training, and the entity is encouraged to offer similar training to staff (Art 20(1) and 20(2)).
- Take appropriate and proportionate technical, operational and organisational measures to manage the risks to the network and information systems it uses, and to prevent or minimise the impact of incidents on recipients of its services (Art 21(1)).



- Base those measures on an all-hazards approach and cover at least the ten items in Art 21(2): risk analysis and information system security policies (a), incident handling (b), business continuity, backup and crisis management (c), supply chain security (d), security in acquisition, development and maintenance including vulnerability handling and disclosure (e), assessment of the effectiveness of the measures (f), basic cyber hygiene and cybersecurity training (g), cryptography and encryption (h), human resources security, access control and asset management (i), and multi-factor authentication and secured communications (j).
- Take into account, for supply chain risk, the vulnerabilities specific to each direct supplier and service provider and the overall quality of their products and cybersecurity practices (Art 21(3)).
- Notify significant incidents in stages (Art 23): an early warning within 24 hours (Art 23(4)(a)), an incident notification within 72 hours updating that warning with an initial assessment of severity and impact and, where available, indicators of compromise (Art 23(4)(b)), and a final report within one month (Art 23(4)(d)).
- Provide the competent authority, on request, with information and evidence of implementation of its cybersecurity policies (Art 32(2)(e) to (g) for essential entities, Art 33(2)(d) to (f) for important ones).

4.1.5 Network Code on Cybersecurity (NCCS)

The Network Code on Cybersecurity (Commission Delegated Regulation (EU) 2024/1366), published in March 2024, is a delegated act supplementing the Electricity Regulation (EU) 2019/943 that aims to create a European baseline for the cybersecurity of cross-border electricity flows. Article 2(1) lists the entity types the regulation can reach.

An identified entity must:

- Perform cybersecurity risk management every three years for all assets in its perimeters (Art 26(2)), identifying risks from assets, threats including supply chain threats, vulnerabilities including in legacy systems, attack scenarios and existing controls (Art 26(4)(a)(i) to (vi)), analysing likelihood and consequences on a common risk impact matrix (Art 26(4)(b)), classifying assets and defining the perimeters through a business impact assessment using the ECII (Art 26(4)(c)(i) to (iv)), setting a mitigation plan with residual risks (Art 26(5)) and deciding whether to accept them (Art 26(6)). Results go to the competent authority within 12 months of notification, then every three years (Art 27).
- Establish a cybersecurity management system within 24 months of notification, covering scope, senior management involvement, a documented cybersecurity policy, roles, entity-level risk management, documented information, performance evaluation, internal audits and review of implementation (Art 32(1)(a) to (l)).
- Apply the minimum and advanced controls within 12 months of their approval (Art 29(6)), plus the supply chain controls, which span the lifecycle of ICT products, services and processes in the perimeters and set procurement specifications on traceability, security updates, audit rights and supplier risk profile (Art 33(2)(a)(i) to (x)).



- Establish at least the CSOC capabilities for the perimeter: security logging enabling anomaly detection, monitoring including intrusion detection and vulnerability assessment, analysis and protective action, and participation in information sharing (Art 38(1)(a)(i) to (iv)), which may be procured from MSSPs without transferring responsibility (Art 38(1)(b)). Reportable cyber-attacks, meaning those classified high or critical on the cyber-attack classification scale, go to the CSIRT and competent authority within four hours (Art 38(3) and 38(4)); unpatched actively exploited vulnerabilities (Art 38(5)) and cross-border cyber threats (Art 38(6)) go to the CSIRT.
- Identify, classify and respond to cyber-attacks affecting cross-border flows (Art 39(1)) through management procedures setting out roles, tasks and reactions based on the observable evolution of the attack (Art 39(3)(c)), tested annually (Art 39(3)(d)), and run exercises: critical-impact entities by 31 December of the year after notification and every three years after (Art 43(1)), and regional or cross-regional exercises from 31 December 2029 (Art 44(1)), with organisers reporting the outcome (Art 45(2)).

4.1.6 Critical Entities Resilience (CER) Directive

The CER Directive (Directive (EU) 2022/2557), published in December 2022 and currently being transposed into national law, aims to strengthen the resilience of critical entities against non-cyber threats such as physical, natural and insider risks, complementing the cybersecurity focus of NIS2.

A designated critical entity must:

- Carry out a risk assessment within nine months of notification, then whenever necessary and at least every four years, on the basis of the Member State risk assessment under Article 5 and other relevant sources, to assess all relevant risks that could disrupt the provision of its essential services (Art 12(1)).
- Account in that assessment for all relevant natural and man-made risks that could lead to an incident, including risks of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies, hybrid threats and other antagonistic threats including terrorist offences, and take dependencies on and from other sectors into account (Art 12(2)).
- Take appropriate and proportionate technical, security and organisational measures to ensure its resilience, based on the Member State risk assessment and on the outcome of its own (Art 13(1)), including measures to prevent incidents from occurring, considering disaster risk reduction and climate adaptation (a); ensure adequate physical protection of premises and critical infrastructure, considering fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls (b); respond to, resist and mitigate the consequences of incidents, considering risk and crisis management procedures, protocols and alert routines (c); recover from incidents, considering business continuity measures and the identification of alternative supply chains (d); ensure adequate employee security management, considering categories of personnel exercising critical functions, access rights, background checks, and training



requirements and qualifications (e); and raise awareness of measures (a) to (e) among relevant personnel through training courses, information materials and exercises (f).

- Describe those measures in a resilience plan or equivalent documents (Art 13(2)) and designate a liaison officer or equivalent as the point of contact with the competent authority (Art 13(3)).
- Notify incidents that significantly disrupt or could significantly disrupt the provision of essential services, with an initial notification no later than 24 hours after becoming aware and a detailed report no later than one month thereafter (Art 15(1)).
- Provide the competent authority, on request, with the information needed to assess whether its measures meet Article 13 and with evidence of their effective implementation, including the results of an audit by an independent qualified auditor (Art 21(2)(a) and (b)). Competent authorities may also conduct on-site inspections and off-site supervision and conduct or order audits (Art 21(1)).

4.2 Standards

Standards and their choices depending on the final application were researched during Task 6.5. As different standards address different aspects of cyber security, the standards considered in the gap analysis have been grouped into three main categories:

- **Security Framework Standards such as ISO 27019 and IEC 62443.** These standards are used by organizations to structure and organize their security and can usually be certified against. Organizations seek or need compliance towards regulations and find that through compliance to or certification against these framework security standards.
- **Communication Standards.** These standards form the backbone of an OT network. Some security controls (i.e., encryption and message authentication) are relevant for interoperability. Therefore, this is usually part of a communication standard, though details are usually covered by technical standards. Most standards we consider here are higher level standards that utilize other standards which are lower in the ISO/OSI model (e.g., Modbus building on TCP-IP).
- **Technical standards.** These standards (e.g., the AES standard) cover device security, access control, and similar aspects. There are usually generic solutions for very focused tasks, and comparatively few are specially made for OT systems.

The standards considered in Task 6.5 are presented and described in Section 5.2 and ANNEX V presents an extensive list of relevant OT Communication Protocols.



5 Gap analysis

This section presents the gap analysis performed against the regulations and standards identified in the previous chapters. It assesses the extent to which the eFORT KERs comply with relevant regulatory requirements and supports the implementation of cybersecurity standards, while identifying remaining gaps, challenges, and opportunities for improvement.

5.1 Regulations

5.1.1 KERs that are compliant with grid security regulations

This section presents an analysis of how the relevant project's KERs are compliant with the relevant grid security regulations.

As a part of the analysis conducted in Task 6.6, a survey was sent to the task leaders to understand which KERs would need to comply with cybersecurity regulations, and how. The complete questionnaire is provided in ANNEX I.

Table 5-1 provides an overview of KERs and their status regarding compliance to regulations. Not all of the project's KERs listed in Table 3-1 appear here. The table covers only those KERs whose solutions could face compliance obligations under one or more of three regulations: the General Data Protection Regulation (GDPR), the Artificial Intelligence Act (AI Act), and the Cyber Resilience Act (CRA). The remaining KERs are not assessed here, as their outputs do not fall within the scope of these three frameworks. The following paragraphs explain in more detail these results.

Table 5-1. KERs and their compliance status with grid security regulations

KER	KER Name	GDPR	AI Act	CRA
1	eFORT Intelligent Platform	Compliant	Does not need to comply	NA
3	Secure Box	NA	NA	Needs to comply
7	Islanding Operation Module	Compliant	NA	NA
8	IDS (Intrusion Detection System)	Compliant	NA	Needs to comply
9	SIEM (Security Information and Event Management)	NA	NA	Needs to comply
10	Chatbot	NA	Does not need to comply	NA



KER	KER Name	GDPR	AI Act	CRA
12	RTU (Remote Terminal Unit)	NA	NA	Needs to comply
14	SOAR (Security Orchestration, Automation and Response)	NA	NA	Does not need to comply

5.1.1.1 General Data Protection Regulation (GDPR)

For several KERs, feedback was received that data is processed but not personal nor sensitive data, which means the GDPR imposes no requirements on these KERs.

According to the questionnaire, GDPR obligations arise for KER 1 (eFORT Intelligent Platform), KER 8 (IDS) and KER 7 (Islanding Operation Module).

The Intelligent Platform (KER 1) processes structured technical data from grid components such as RTUs and IDS logs: timestamps, device IDs, event types, anomaly indicators. No personal customer data is collected by design. Any GDPR-relevant data is anonymised. Data travels through encrypted VPN tunnels, authenticated with HMAC-SHA-256, and is stored in access-controlled environments with role-based access control. Access logs and audit mechanisms support accountability

The Islanding Operation Module (KER 7) processes measurements, estimations and calculated values for grid power and voltage. This becomes personal data if it can be linked to individual customers or their usage patterns (Art 4(1), Recital 26). Where it is, the DSO acts as controller and carries responsibility for lawfulness and security. The data stays inside EDYNA's facilities, since the T5.4 platform runs on the DSO's local LAN. Names and identifying details are redacted before any external presentation or publication.

The IDS (KER 8) detects suspicious activity across the network and equipment using host-based and network-based intrusion detection. The data it reads can include personal data, since IP addresses and user accounts qualify (Art 4(1), Recital 30). Reading and analysing data is itself processing (Art 4(2)), so the GDPR applies even though no data is retained. The task leader reported that data is not stored, which is a sound data-minimisation and storage-limitation measure (Art 5(1)(c) and (e)), and access to processed information is limited to registered users, an appropriate Article 32 measure.

5.1.1.2 Artificial Intelligence (AI) Act

The tools developed in the eFORT project are AI systems used as supporting tools within the electricity grid, but they have no direct management or operational impact on it. They are, therefore, not safety components in the sense of Annex III, point 2, and fall outside the high-risk category. As limited or minimal-risk AI systems, none of the KERs is required to meet the AI Act's cybersecurity requirements.



The Intelligent platform (KER 1) uses unsupervised machine-learning models for anomaly detection, in particular clustering and statistical outlier detection. These features also fall under the low-risk category and so are not required to meet cybersecurity requirements.

The Chatbot (KER 10) provides conversational access to grid status and includes an integrated alert system, built on the LangChain framework and LLMs. These features fall under the low-risk category, so no cybersecurity obligation applies. One qualification: a chatbot that interacts directly with users is still caught by the transparency duty in Article 50(1), which requires informing users that they are dealing with an AI system unless that is obvious from the context. The task leader reported in the questionnaire that clear documentation and technical controls were being implemented, which goes beyond what the AI Act requires.

5.1.1.3 Cyber Resilience Act (CRA)

None of the eFORT KERs is currently placed on the market, so the CRA does not yet apply to any of them. The analysis below sets out what would follow on commercialisation.

The Secure Box (KER 3) performs cryptographic operations and secure key storage through a dedicated secure element (Microchip ATECC608A/B) for authentication, encryption and key management. It includes hardware anti-tampering mechanisms, using an integrated accelerometer for motion and tamper detection, and is a multi-component hardware device with VPN-secured communications, secure update mechanisms and protected data handling at the edge. If commercialised, it would most likely be a critical product under Annex IV, point 1, "hardware devices with security boxes": hardware that securely stores or processes sensitive data or performs cryptographic operations and incorporates a physical envelope providing tamper evidence, resistance or response. Therefore, the Secure Box could face the strictest CRA route if commercialised.

The IDS (KER 8) would be an important product, Class II (Art 7(1), Annex III, Class II, point 2, covering firewalls and intrusion detection and prevention systems). Recital 45 confirms that intrusion detection and prevention systems sit in Class II and are subject to mandatory third-party conformity assessment. Independent verification via a notified body would therefore be unavoidable, with no self-assessment route.

The SIEM (KER 9) would be an important product, Class I (Art 7(1), Annex III, Class I, point 7, "security information and event management (SIEM) systems"). Self-assessment under internal control remains available, but only if the manufacturer applies harmonised standards, common specifications or a certification scheme covering all the essential requirements.

The RTU (KER 12) would fall in the default category and would have to meet the essential cybersecurity requirements in Annex I Part I and the manufacturer processes in Annex I Part II, demonstrated through self-assessment under Module A. This holds provided the RTU's core functionality is not network management (Annex III, Class I, point 6) and it does not qualify as a microcontroller with security-related functionalities (point 14), either of which would escalate it to Class I.



The SOAR (KER 14) falls outside the CRA. It is free and open-source software, not monetised and not made available on the market in the course of a commercial activity (Recital 18). If that changed, it would come into scope and, depending on its core functionality, could land in the default or important category.

5.1.2 KERs that contribute to the fulfilment of grid security regulations

This section presents the analysis of how the relevant project's KERs can contribute to the fulfilment of selected grid security regulations. For each KER, the relevant provisions of the applicable regulations were identified and mapped against the expected capabilities or outputs of the KER.

To validate this mapping, a survey was sent to the task leaders associated with the tasks contributing to each KER. This final evaluation gathered the opinions of the task leaders on whether and how the identified KERs could support the selected regulatory requirements. The complete questionnaire, including the texts of the regulatory articles assessed, is provided in ANNEX I.

Table 5-2 provides an overview of the resulting assessment, while the following paragraphs explain in more detail how each KER can contribute to the relevant regulatory articles. Not all of the project's KERs listed in Table 3-1 appear here. The table covers only those KERs whose solutions could help end users meet obligations of one or more of the following EU regulations: the Network and Information Security Directive (NIS2), the Network Code on Cybersecurity (NCCS), the Critical Entities Resilience Directive (CER). The remaining KERs are not assessed here, as their outputs would not contribute to the fulfilment of these regulatory frameworks.

Table 5-2. KERs supporting EU regulations

KER	KER Name	NIS2	NCCS	CER	CRA
1	eFORT Intelligent Platform	Articles 21(1), 21(2)(a) and (b), 23(4)(b), 29(1) (a) and (b)	Articles 38(1)(a)(iv), 38(6), 39(1), 39(3)(c)	Articles 10(2), 10(3), 12(1), 12(2), 13(1), 13(1)(a), 15(3)	
2	Data Base Tool	Articles 21(1), 21(2)(e)	Articles 26(4)(a)(i) to (vi), 38(1)(a)(i) and (ii)	Articles 13(1)(a) and (c), 21(2)(a) and (b)	
3	Secure Box	Articles 21(1), 21(2), 21(2)(i), 21(2)(c)	Articles 26(4)(a)(iii), 26(4)(c)(iv)	Article 13(1)(a)	
4	Training (CRoF + Digital Twin)	Articles 20(2), 21(1), 21(2)(g)	Articles 43(1), 44(1), 45(2)	Articles 10(1), 13(1)(e), 13(1)(f)	Recital 23



KER	KER Name	NIS2	NCCS	CER	CRA
6	Dynamic Risk Assessment Tools	Articles 21(2), 21(2)(a)	Article 26(4)(a)(i) and (c)(iii) to (iv), 26(4)(b)	Articles 12(1), 12(2)	
8	IDS (Intrusion Detection System)	Articles 21(1), 21(2)(b), 23(4)(b)	Articles 32(1)(i) to (k), 38(1)(a)(i), 38(1)(a)(ii), 39(1)		
9	SIEM (Security Information and Event Management)	Articles 21(2)(b), 23(4)(b), 32(2)(e) to (g), 33(2)(d) to (f)	Articles 38(1)(a)(i), 39(1)		
10	ChatBot	Article 21(2)(a) Partially: 21(1)	Articles 39(1), 38(1)(a)(iii)		
11	Guide for safe design of substations	Articles 21(2)(e), 21(2)(f), 32(2)(e) to (g), 33(2)(d) to (f) Partially: 21(2)(a)	Articles 28(2), 28(3), 29(6)	Articles 13(1)(a), 13(1)(c)	
12	RTU (Remote Terminal Unit)	Article 21(1)	Article 39(1)		
13	Blockchain for grid resiliency	Articles 21(2)(d), 21(3), 21(2)(a), 21(2)(b)	Articles 33(2)(a)(vii) to (x), 39(1)	Article 13(1)(a), (c) and (d)	
14	SOAR (Security Orchestration, Automation and Response)	Articles 21(2)(b), 21(1)	Articles 38(1)(a)(iii)		
15	Blueprint for EPES SOC infrastructure	Articles 21(2)(b), 21(1)	Articles 38(1)(a)(i) to (iv), 38(3)		



KER	KER Name	NIS2	NCCS	CER	CRA
21	Connected devices vulnerabilities	Articles 21(2)(e), 21(2)(d), 21(3) Not supported: 12(1) and 12(2)	Articles 26(4)(a)(i) to (iv), 26(5) to (6), 38(5)	Articles 12(1) and 12(2)	Article 6(b) and Annex I, Part II, points 1 to 8

5.1.2.1 eFORT Intelligent Platform (KER 1)

This KER supports NIS2, the NCCS and CER by improving monitoring, anomaly detection, alerting, visualisation and information sharing.

- For NIS2, it supports Article 21(1) by helping operators detect incidents earlier and reduce their potential impact, while also supporting risk analysis and incident handling under Article 21(2)(a) and Article 21(2)(b) through timely and structured operational information. Its alerts, event data, timestamps and potential indicators of compromise can also support incident reporting under Article 23(4)(b), by helping operators assess severity and impact of an incident, and voluntary cybersecurity information sharing under Article 29(1)(a) and (b) by enabling the exchange of relevant data.
- For similar reasons, regarding the NCCS, the platform supports CSOC information collection and sharing under Article 38(1)(a)(iv), cyber-threat information sharing under Article 38(6), and the identification, classification and response to cyber-attacks under Article 39(1). Its interactive visualisation tool also supports Article 39(3)(c) by helping operators follow the observable evolution of an attack and select appropriate reaction tasks within predefined cyber-attack management procedures and roles.
- For CER, it supports risk assessment under Article 12(1) and Article 12(2), resilience and incident prevention measures under Article 13(1) and Article 13(1)(a), and cooperation or information sharing under Article 10(2), Article 10(3) and Article 15(3).

5.1.2.2 Data Base Tool (KER 2)

The tool supports NIS2, the NCCS and CER by improving vulnerability visibility, risk prioritisation, monitoring support and evidence generation for EPES infrastructure.

- For NIS2, it supports the obligation to take appropriate cybersecurity risk-management measures under Article 21(1), and security in acquisition, development and maintenance, including vulnerability handling, under Article 21(2)(e), by linking vulnerability intelligence with EPES-specific asset, exposure, criticality, mitigation and patch information.
- For the NCCS, it supports entity-level cybersecurity risk assessment under Article 26(4)(a)(i) to (vi) by combining assets, vulnerabilities, threats, attack scenarios,



security events and possible controls, and supports CSOC capabilities for monitoring, intrusion detection and vulnerability assessment under Article 38(1)(a)(i) to (ii), especially when integrated with SIEM and IDS components.

- For CER, it supports incident-prevention measures under Article 13(1)(a), response and mitigation of incident consequences under Article 13(1)(c), and the provision of information or evidence to competent authorities under Article 21(2)(a) and (b), through records of vulnerabilities, patch status, alerts and risk outputs.

5.1.2.3 SecureBox (KER 3)

The tool supports NIS2, the NCCS and CER by strengthening local access control, asset protection and substation resilience.

- For NIS2, it supports Article 21(2)(i) by helping enforce access restrictions and protect substation assets from unauthorised use, while also contributing to Article 21(1) by containing local compromise and reducing the risk of wider disruption. Its protection against physical tampering supports the all-hazards approach under Article 21(2), and its ability to maintain substation protection and monitoring during communication disruptions contributes to continuity and crisis management under Article 21(2)(c).
- For the NCCS, SecureBox supports perimeter definition and access control under Article 26(4)(c)(iv) by helping enforce and evidence local security boundaries at substation or microgrid level and supports Article 26(4)(a)(iii) by reducing tampering-related vulnerabilities that could enable cyber compromise of substation ICT assets.
- For CER, it supports Article 13(1)(a) by helping prevent physical manipulation and reducing the likelihood of incidents affecting substation assets and service continuity. However, the final evaluation highlighted that it does not support adequate physical protection of premises and critical infrastructure as of Article 13(1)(b). That is due to the fact that SecureBox mainly protects the device itself rather than the wider premises or critical infrastructure, which would require broader physical protection measures.

5.1.2.4 CRoF training and digital twin environment (KER 4)

The training and the digital twin support NIS2, NCCS, CRA, and CER by strengthening cybersecurity training, awareness, incident preparedness and resilience exercises in realistic power-grid contexts.

- For NIS2, it supports basic cyber hygiene and cybersecurity training under Article 21(2)(g), incident-impact reduction under Article 21(1), and management awareness under Article 20(2) by helping operators, cybersecurity staff and relevant management personnel practise detection, coordination, mitigation, recovery and risk-based decision-making.
- For the NCCS, it supports periodic cybersecurity exercises under Articles 43(1) and 44(1), as well as exercise outcome reporting under Article 45(2), by providing



realistic TSO/OT scenarios, operator workflows, digital-twin analysis, KPIs, action logs, debrief inputs and lessons learned.

- For the CRA, it supports the cybersecurity skills described in Recital 23 by training staff in monitoring, incident handling and coordinated response.
- For CER, it supports awareness raising under Article 13(1)(f), employee training and qualification aspects under Article 13(1)(e), and resilience exercises under Article 10(1) by exposing personnel to realistic attack paths, operational impacts, mitigation choices and recovery actions.

5.1.2.5 Dynamic Risk Assessment Tools (KER 6)

The tools support NIS2, NCCS and CER by strengthening cyber-physical risk assessment, disruption-impact analysis and the prioritisation of risk mitigation measures, although their contribution differs by tool component.

- For NIS2, both components can support the all-hazards approach and risk-analysis and information-system-security policies under Articles 21(2) and 21(2)(a), as they both enable the assessment of physical hazards. The Dynamic Security Assessment tool can also analyse the consequences of outages, including those potentially triggered by cyberattacks, while geo-referenced hazard quantification constitutes a key input for the risk assessment.
- For the NCCS, the geo-referred asset/location view can support risk ranking and asset prioritisation by helping identify assets, assess their potential impact on cross-border electricity flows, and determine high-impact and critical-impact perimeters, as laid out in Article 26(4)(a)(i) and 26(4)(c)(iii)–(iv). The Dynamic Security Assessment tool also supports Article 26(4)(b) by assessing the consequences of disruption events resulting from cyberattacks and helping determine risk levels through a risk impact matrix.
- For CER, the Dynamic Security Assessment tool supports the periodic risk assessment of relevant disrupting risks under Article 12(1) by evaluating the potential impact of disruption scenarios on critical infrastructure. By integrating climate data with physical risk assessment capabilities, the tool also contributes to an all-hazards methodology covering natural disasters and cross-border dependencies under Article 12(2).

5.1.2.6 IDS (KER 8)

The tool supports NIS2 and the NCCS by strengthening security monitoring, early incident detection, incident handling and response prioritisation.

- For NIS2, it supports incident handling under Article 21(2)(b) by detecting suspicious activity, helping identify potential incidents early, assessing their scope and supporting containment or remediation actions. It also supports incident-impact reduction under Article 21(1), since faster detection and triage can help organisations understand incidents earlier, prioritise response and reduce operational, financial and security impact. In addition, IDS outputs can support incident notification under Article 23(4)(b) by providing relevant information such



as affected systems, alert severity, timestamps, attack indicators and indicators of compromise.

- For the NCCS, the IDS supports CSOC monitoring and intrusion detection under Article 38(1)(a)(ii), security logging, anomaly detection and cyber-attack analysis under Article 38(1)(a)(i), and the identification, classification and response to cyber-attacks affecting cross-border flows under Article 39(1). Its configurable and updatable detection rules also support performance evaluation and continual improvement under Article 32(i) to (k), by enabling tuning, documentation, effectiveness reviews and audit evidence.

5.1.2.7 SIEM (KER 9)

The tool supports NIS2 and the NCCS by providing a centralised capability to collect, aggregate, correlate and analyse security-relevant information from IT and OT assets.

- For NIS2, it supports Article 21(2)(b) by strengthening incident handling through improved detection, triage and investigation of security events. It also supports Article 23(4)(b) by helping produce incident notification content, including an initial assessment of severity, impact and, where available, indicators of compromise. SIEM data and reports can further provide evidence of implementation for competent-authority audits and supervision under NIS2 Articles 32(2)(e) to (g) and 33(2)(d) to (f).
- For the NCCS, a cloud SIEM supports Article 38(1)(a)(i) by centralising security logs for monitoring and anomaly detection, and supports Article 39(1) by helping investigate, classify and document cyber-attacks.

5.1.2.8 Chatbot (KER 10)

The tool supports NIS2 and the NCCS by improving operators' access to monitoring and security information, thereby contributing to situational awareness, risk management and incident-response support.

- For NIS2, it can support policies on risk analysis and information system security under Article 21(2)(a) by making relevant monitoring information easier to access and helping operators build a more complete operational picture. It can also contribute to incident-impact reduction under Article 21(1), although more indirectly, by allowing users to quickly query asset status and monitoring information during potential incidents.
- For the NCCS, the chatbot supports the identification, classification and response to cyber-attacks affecting cross-border flows under Article 39(1), as well as the CSOC capability to analyse and take protective action under Article 38(1)(a)(iii), by providing natural-language access to IDS-generated alerts and security information. By lowering the friction of consulting monitoring data, the chatbot can improve operator responsiveness and support faster analysis during cybersecurity events.



5.1.2.9 Guide for safe design of substations (KER 11)

The secure-by-design substation guidelines and accompanying testbook support NIS2, the NCCS and CER by strengthening secure substation design, risk and vulnerability management, cybersecurity verification and incident detection capabilities.

- The guidelines support NIS2 Article 21(2)(e) by contributing to secure acquisition, development and maintenance of substations, including vulnerability handling, and may also support Article 21(2)(a) where adapted to a common risk-analysis methodology. The testbook supports NIS2 Article 21(2)(f) by verifying the effectiveness of cybersecurity risk-management measures and can provide audit and supervision evidence under Article 32(2)(e) to (g) and Article 33(2)(d) to (f).
- For the NCCS, the guide supports Article 28(2) to (3) and Article 29(6) by helping identify risks and enabling an OT-adapted risk and vulnerability workflow, while its relevance to procurement (Article 35), cybersecurity management-system documentation (Article 32(1)(d), (i) and (l)) and regular audits (Article 32(1)(j) to (k)) is limited because these are not its primary focus.
- For CER, secure-by-design substations support Article 13(1)(a) as an incident-prevention measure through intrusion-detection-oriented results and strongly support Article 13(1)(c) by enabling early malfunction detection, intrusion detection and alarm generation. However, the final evaluation highlighted that they do not support Article 13(1)(b), as this KER is not oriented to physical protection.

5.1.2.10 RTU (KER 12)

The tool supports NIS2 and the NCCS by improving operational visibility and supporting earlier detection of abnormal conditions.

- For NIS2 it can help minimise the impact of incidents on recipients of services by enabling earlier visibility through monitoring, supporting Article 21(1) of NIS2.
- For the NCCS, the RTU trigger-on-change and trigger-on-quality reporting can help detect abnormal behaviour and potential cyber incidents by flagging unexpected changes, communication issues or degraded data quality, while IEC 61850 reports and logs support traceability for incident analysis, supporting Article 39(1).

5.1.2.11 Blockchain for grid resiliency (KER 13)

The blockchain for grid resiliency functions support NIS2, the NCCS and CER by strengthening supply-chain traceability, anomaly detection and operational response planning

- For NIS2, blockchain-based tracing supports supply-chain security under Article 21(2)(d) and 21(3) by creating tamper-evident records of component origin, ownership, supplier involvement and lifecycle events. This helps assess supplier risks, vulnerabilities and product quality. TSO-level consumption monitoring also supports Articles 21(2)(a) and 21(2)(b) by detecting abnormal demand patterns that may indicate cyber incidents, manipulation or operational anomalies, thereby supporting risk analysis, incident triage and impact assessment.



- For the NCCS, blockchain-based tracing supports Article 33(2)(a)(vii)–(x) by providing traceability and audit evidence across development, delivery, updates and supplier actions. TSO-level consumption monitoring also supports Article 39(1) by helping identify unusual operational patterns and classify potential cyber-attacks affecting electricity flows.
- For CER, blockchain-based tracing supports Article 13(1)(d) by helping identify supplier dependencies and potential alternatives for business continuity and recovery planning. TSO-level consumption monitoring also supports Article 13(1)(a) and 13(1)(c) by informing operational responses to prevent, mitigate and recover from incidents affecting critical infrastructure.

5.1.2.12 SOAR (KER 14)

The tool supports NIS2 and the NCCS by automating incident handling, response coordination and protective actions.

- For NIS2, it directly supports incident handling under Article 21(2)(b) by enabling structured and automated response workflows, and incident-impact reduction under Article 21(1), as faster and more consistent response can help limit the operational, security and service impact of incidents.
- For the NCCS, the SOAR supports the CSOC capability to analyse and take protective action under Article 38(1)(a)(iii), by using playbooks and automated response actions to support investigation, containment and mitigation.

5.1.2.13 Blueprint for EPES SOC infrastructure (KER 15)

The blueprint for EPES SOC infrastructure supports NIS2 and the NCCS by helping establish structured, standardised and repeatable incident-handling and security-operations capabilities.

- For NIS2, it supports incident handling under Article 21(2)(b) by defining how alerts, incidents, escalation, containment and remediation processes should be organised. It also supports incident-impact reduction under Article 21(1), since a faster and more consistent SOC setup can improve detection, coordination and response, helping to reduce the operational and security impact of attacks.
- For the NCCS, the blueprint can serve as a concrete reference design for establishing CSOC capabilities under Article 38(1)(a)(i) to (iv), including security monitoring, analysis, vulnerability-related information flows and protective actions. It can also support Article 38(3) by defining the roles, processes and information flows needed to share reportable cyber-attack information within the required timeframe, including through playbook sharing and coordinated incident-response procedures.

5.1.2.14 Connected devices vulnerabilities (KER 21)

The connected-device vulnerability findings support NIS2, the NCCS, the CRA and CER by providing concrete evidence of weaknesses in IoT and connected devices.



- For NIS2, the findings support vulnerability handling under Article 21(2)(e) and can inform supply-chain security under Article 21(2)(d) and Article 21(3) by highlighting vulnerabilities linked to specific products, suppliers or supplier cybersecurity practices. However, they do not by themselves support the coordinated vulnerability disclosure framework under Article 12(1) and Article 12(2), unless a coordinated disclosure process is added around the findings.
- For the NCCS, the findings can feed into entity-level cybersecurity risk assessment under Article 26(4)(a)(i) to (iv), while CVSS scoring can support risk treatment and residual-risk decisions under Article 26(5) and Article 26(6). If an in-scope vulnerability is actively exploited and unpatched, it may also provide relevant information for notification to the CSIRT under Article 38(5).
- For the CRA, the findings can support manufacturers' vulnerability-handling obligations under Article 6(b) and Annex I, Part II, points 1 to 8, since reported vulnerabilities would need to be assessed and addressed by the manufacturer.
- For CER, the findings can contribute to critical-entity risk assessment under Article 12(1) and Article 12(2), especially where the vulnerabilities could affect essential services, connected assets or cascading risks.

5.2 Standards

Standards play several roles that are vital for operation of complex systems. The most straightforward role is interoperability, to assure that devices are replaceable and have a baseline to rely upon when interoperating with different system components. In security, the role is different – technical standards not only have the task of assuring interoperability, but also to help manufacturers and users make appropriate security decision and allow experts to thoroughly review the technologies used by a wide user base – that is (part of) the role of standardized protocols, and more focused technical standards such as encryption or random number generation.

In addition, higher level standards such as ISO 27001 and IEC 62443 give companies a framework to define their security policies and procedures and allow for certification to assure themselves and customers that standards have been met. Ideally, those standards also link into regulation such as NIS 2, so that a company that properly follows the standard has thus also performed best practices as required by the regulator.

On the technical standards, a rather large number of them are applicable and used in the Energy sector, though most do not require a gap analysis due to the high level of specialization. For example, the AES standard is a universal standard used for symmetric encryption and is doing this highly specialized task rather well. If it is not applicable for a specific setting (e.g., for extremely low performant devices), one should deploy a different standard for that particular use case than attempt to amend AES. Gaps in this area are mostly due to some useful technologies not standardized at this point at all.

There are a number of challenges in the standardization process that lead to gaps that make the standards less suitable for secure operations. One reason is the conflict of interest with other goals – security measures can add complexity in implementation and



operation and may thus be reduced to accommodate other needs. Another challenge is that standardization tends to be a slow process, and – especially in the current environment – the electricity grid and threat models are changing at a pace that standard bodies have a hard time keeping up with.

Gaps can be addressed by standards bodies, in the selection of different standards that serve a similar purpose, but also – often more likely – need to be addressed separately, by means unrelated to the standard itself. Residual risk may need to be mitigated through architecture (e.g., zero trust), monitoring, secure operations, or device hardening. Awareness of potential gaps can also help choosing the right standard for the right purpose, as – especially in communication standards – there is a multitude of standards to choose from, with different outcomes on the gap assessment

This section presents the analysis of cyber security standards, and the overarching gaps that are considered applicable to the scope of this assignment following the distinction between Security Framework Standards (Section 5.2.1), Communication Standards, (Section 5.2.2) and Technical standards (Section 5.2.3).

5.2.1 Security Framework Standards

MITRE ATT&CK for ICS. The MITRE ATT&CK for ICS framework is a classification and knowledge base for tactics, techniques, and procedures used against industrial control systems. It follows the general flow of attacks from initial access, execution, persistence, lateral movement, etc., with a focus on OT-related assets. It is not a security standard in itself but can be used to evaluate security controls against typical attack techniques; in this, it adds the attacker focus to standards like IEC 62443. Given its depth, it is a good tool to check an overall architecture and configuration for security gaps.

ISO/IEC 2700x (IT) and ISO/IEC 27019 (energy). These standards are information-security-based framework standards for policies, governance requirements, and security controls. The ISO/IEC 27000 family is the most widely adopted IT security framework, and a large audit infrastructure exists. The framework is a collection of standards, with 27000 giving a general overview, 27001 defining how to set up an ISMS, 27002 defining security controls, etc. The standard is IT-heavy, and often not well fitted for OT systems. Even though the line between those two is blurring, ISO/IEC 2700x is not very good at taking in the extra requirements coming from OT.

The 27019 Standard is one exception here. Essentially, ISO/IEC 27019:2024 provides energy-utility-specific controls based on ISO/IEC 27002, i.e., it aims to propose measures to mitigate risks identified in grid-related systems such as process control, substation automation, DER-related systems, etc. In this, it is more management and policy oriented than the more technical IEC 62443. The newest version, ISO/IEC 27019:2024, is a substantially modernized version, which also adds new relevant issues such as supplier management and anomaly detection, as well as taking into account modern challenges such as DER.

Thus, while 27019 does address the particular requirements of OT environments, it provides only limited technical guidance on how controls should be implemented in practice. For example, in areas such as patch management, network segmentation, and secure remote access, the standard primarily defines governance expectations and risk



management principles rather than detailed technical requirements. As a result, organizations relying solely on 27019 may face gaps in the specification of concrete security measures, testing procedures, and system-level controls. These aspects are addressed in considerably greater depth by IEC 62443. ISO 27019 is best viewed as a complementary governance and control-selection standard that supports security governance in the electricity sector, while more detailed technical standards are required to fully address OT cybersecurity requirements. Unsurprisingly, the standard also struggles to keep up with the rapid development in the new threat models, security approaches, and the evolving grid infrastructure.

IEC 62443. IEC 62443 is a framework standard for OT systems. It is a family of standards that covers multiple topics, including a reference on assessing gaps in communication standards. At the same time, IEC 62443 also has its own gaps, e.g., not sufficiently taking into account resource constraints, implementation issues and real-time requirements. Resource constraints include CPU capability, bandwidth restrictions, memory limits, but may also include lack of proper I/O or operating system features. Implementation and operational problems include safety, maintainability, physical hardening requirements that require specialized hardware, devices being difficult to physically reach or protect, and long lifetimes of the devices; they also include the inability to run additional software on the devices, warranty restrictions, and the inability to patch without a careful assessment of the consequences. Real-time requirements are a special case of operational requirements, which often also do not allow for additional hardware or functionality. Thus, the approach also seen in ISO 2700x to resolve security risks by adding controls can have severe side effects in OT systems. Furthermore, due to the origin of a more production-oriented OT, IEC 62443 does not always sufficiently take into account the distributed nature of especially energy OT systems, assuming both a limited geographic scope and an asset owner with a large degree of control over all digital assets. Like ISO 2700x and other standards, it also suffers from the naturally slow pace of standard development, which makes it hard to react to modern threats.

62443 is comprehensive and covers among others system architecture and device security. It is the most comprehensive OT cybersecurity framework among the standards considered here and therefore chosen as a reference to measure communication standards against. As examples we mention the issue of key management or secure software updates: each lower-level standard can define this as 'out of scope' rather than a gap, which leads to gaps in the overall system since no individual standard feels responsible for such gaps. IEC 62443 as the most comprehensive framework is the one standard we can hold responsible for this.

Technical working groups related to IEC 62443 and the CRA are working on harmonizing the standardization with the regulation, but no guidelines or alignment work has been published as of yet. These developments would strengthen the alignment of IEC 62443 with the European regulatory landscape and make it a more suitable benchmark for assessing technical cybersecurity capabilities in critical infrastructure environments (CENELEC).

IEEE C37.240. This standard provides cybersecurity requirements specifically tailored to substation automation, protection, and control systems. Like 62443, C37.240 focuses on technical and engineering requirements, but with a much narrower focus. Its limited



scope does not provide the comprehensive system architecture, security-level methodology, and lifecycle requirements found in IEC 62443. Consequently, C37.240 can be viewed as a valuable sector-specific complement to IEC 62443 rather than a replacement for a broader OT cybersecurity framework.

5.2.2 Communication Standards

In this section, Communication Standards are also referred to as Communication Protocols.

5.2.2.1 Reference Standards for Communication Protocols

ISO/OSI layers and the Purdue Model. In the IT world, communication protocols can be layered in the ISO-OSI model, which layers different roles in the protocol, from the physical layer up to the application layer. Security is relevant for the different layers with different properties and addressing different threats. For example, application layer security (such as https) provides security on the highest layer ignoring everything below. This layer is well suited to handling issues such as user authentication, but not very good at handling threats such as a denial-of-service attack or routing-spoofing.

Though many OT protocols build on TCP/IP and thus would be able to reuse their security and treats approach, the layers and responsibilities are not always easily distinguishable and might even be duplicated, making a structured approach to security in this setting somewhat harder.

Another lens to assess protocol security is the Purdue zoning model. Rather than focusing on protocol security itself, this model considers how assets are connected and which security controls are applied at zone boundaries. In this context, a protocol such as Modbus generally assumes that all assets within the same zone are trusted, meaning that the protocol does not need to provide full protection against those assets. Instead, the trust model relies on boundary protection, such as firewalls, to isolate zones and protect devices using insecure protocols from assets they should not trust. Although the Purdue model remains a common reference architecture for OT systems, many practical implementations deviate from it because of specific requirements such as remote maintenance, time synchronization, market integration, and vendor constraints. The zones can be mapped to five levels (*Level 1*: RTU / PLC, *Level 2*: SCADA, *Level 3*: OT Operations, *Level 4*: Business Systems, *Level 5*: Enterprise/Cloud). For the purposes of this report, Levels 3 to 5 are the most relevant.

In general terms, the Purdue model provides a useful high-level reference architecture for OT networks, and it can help illustrate typical communication paths, network zones, firewalls, and demilitarized zones (DMZs). This approach is highly relevant in the OT area for several reasons; for one, OT environments are more vulnerable, and a DMZ with approaches such as jump-hosts is a vital component in allowing some remote maintenance and data transfer while protecting the OT system. Furthermore, some OT environments have vulnerabilities that are extremely difficult to mitigate directly (e.g., slow application of patches and updates), which makes meaningful isolation more relevant. Thirdly, a well implemented DMZ can allow the OT domain to temporarily go into island mode without losing major functionality (as well as reconnect with reasonably



low effort), allowing for a fast reaction to (perceived) threats that otherwise wouldn't be an option. Real-world architectures often differ from the reference model because of legacy systems, vendor requirements, remote maintenance needs, time synchronization, and market integration. Electrical engineers often use the single-line diagram as equivalent reference point. The Purdue model can be useful to map communication protocols to the relevant OT levels and network boundaries. Figure 1 presents a graphical comparison between the two models.

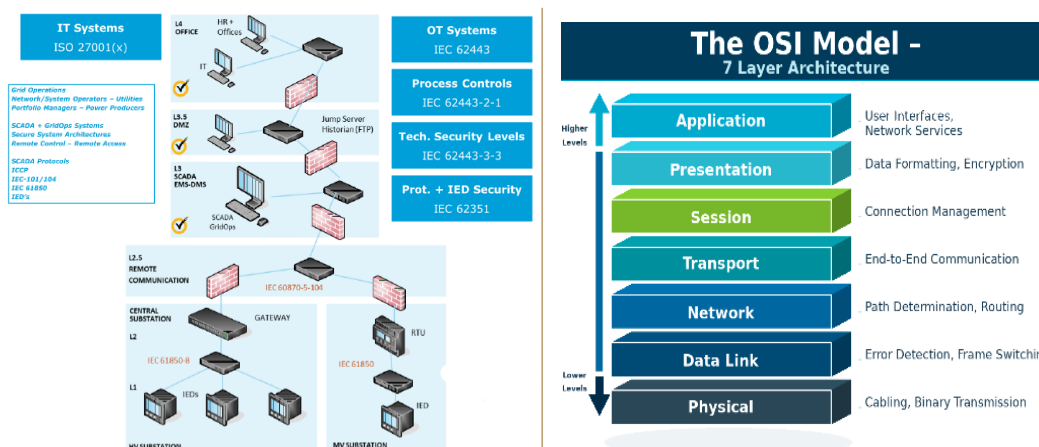


Figure 1. Representation of Purdue Model (left) and OSI model (right) (Kruimer, 10 June 2026)

In more modern IT scenarios, there is the concept of Zero trust. One can (partially) envision that as: the firewall moves from the zone boundaries into the zone itself and also controls communication between devices. This is a powerful concept but adds additional problems for OT systems that hinder easy deployment. These include incomplete knowledge of assets and communication patterns, the risk of the firewall becoming a single point of failure, and an architecture that relies on broadcast communication and therefore does not lend itself to micro segmentation.

The electric grid networks host a variety of protocols, some for vendor specific and historic reasons, some specially designed for their use case. System internal protocols (e.g. in Power plants, Solar/wind/batteries/EMS, etc.) are often the classical industrial protocols such as Modbus, CAN bus, MQTT or OPC UA. In substation automation, common protocols are IEC 60870-5-104, which is increasingly replaced by IEC 61850. Smart metering adds another host of protocols (such as DLMS/COSEM), while the control room relies more on internet protocols.

The ISO 7-layer architecture, formally known as the OSI (Open Systems Interconnection) model, is a conceptual framework that standardizes how data is communicated across a network by dividing the process into seven distinct layers. These layers, Physical, Data Link, Network, Transport, Session, Presentation, and Application, each define specific functions, from transmitting raw bits over physical media to providing end-user services such as file transfer and email. By separating networking tasks into layers, the OSI model promotes interoperability between different systems and vendors, simplifies network design and troubleshooting, and provides a common reference for understanding and developing communication protocols, even though real-world networks often implement a simplified version of this model.

The OSI (ISO 7-layer) model and the Purdue model serve complementary, with the Purdue model defining the hierarchical segmentation of IT/OT environments with the placement of zones and boundaries and the OSI model governs how communication occurs within and across these layers enforcing communication controls across those boundaries through standardized protocol layers. For example, the Purdue model is applied in substation architectures to structure security zones and enforce vertical segmentation, including the use of DMZs and centralized SCADA systems, whereas cybersecurity controls are implemented using OSI-layer mechanisms (e.g. Layer 3–4 traffic filtering or Layer 7 application inspection).

Relevant Resilience Properties for communication protocols. Traditional information security standards such as ISO 27001 are largely built around the CIA triad of Confidentiality, Integrity, and Availability. While these principles are appropriate for enterprise IT environments, operational technology and power system environments are centered around the process- rather than information security, which needs different view on requirements than captured by the CIA model.

In grid operations and other OT processes, one approach is to simply change the priority to AIC, highlighting that Availability and Integrity are substantially more relevant than confidentiality. Another approach is to take a process centric view, and associate process security more closely with maintaining Control, Observability, and Operations (COO). The primary objective is not merely the protection of information, but the safe and reliable operation of the electrical system. Consequently, cybersecurity controls must be evaluated not only with respect to their impact on confidentiality, integrity, and availability, but also regarding their effects on operational performance and system stability.

Several system characteristics that are critical in OT environments receive limited attention in traditional information security standards. These include reliability, maintainability, integrability, and debuggability of field devices and control systems. Similarly, performance-related requirements such as throughput, latency, and deterministic communication behavior are often of equal importance to security requirements. Security mechanisms that introduce excessive processing delays, communication overhead, single points of failure, or operational complexity may negatively impact critical grid functions.

Denial-of-Service (DoS) resilience represents a particularly important consideration. Many industrial communication protocols were designed primarily for trusted environments and may exhibit asymmetric resource consumption characteristics. For example, within IEC 61850 a single GetDataDefinition request can trigger a response of several megabytes, causing substantially greater computational and network load on the responding device than on the requesting device. Such protocol characteristics can potentially be exploited to degrade system performance or availability without requiring high attack bandwidth.

The treatment of confidentiality also differs between IT and OT environments. Confidentiality is typically achieved through symmetric cryptographic algorithms, with the Advanced Encryption Standard (AES) representing the current industry's best practice for protecting communications and stored data. However, in many operational contexts, confidentiality requirements may be secondary to maintaining system availability and operational continuity.



Additional threats that require explicit consideration include replay attacks, in which legitimate communications are captured and retransmitted to trigger unauthorized actions. Protection against such attacks generally requires mechanisms beyond simple encryption, including sequence numbers, timestamps, or cryptographic freshness guarantees.

A further distinction must be made between authentication and integrity. Authentication establishes the identity of a communicating entity, whereas integrity mechanisms provide assurance that transmitted data has not been modified. While the two concepts are often implemented together through cryptographic protocols, they address different security objectives and should be evaluated separately during requirements analysis. Failure to distinguish between authentication and integrity may result in incomplete security controls or incorrect assumptions regarding system protection.

IEC 62443 Requirements on communication protocols. IEC 62443 does define security objectives that systems/components, and therefore the protocols connecting them, should support. Usually (almost always) no protocol can satisfy all requirements, requiring some properties to be mitigated by the overall architecture or other means. In this assignment, IEC 62443 is considered as the main reference over ISO 27019, as the ISO standards are more governance and procedure related, while 62443 also includes more engineering focused parts (such as 62443-3-3) and therefore a better match for communication protocols. It must be noted that IEC 62443 is mostly a generic controls systems standard. This standard has therefore difficulties capturing more modern developments in the grid such as distributed energy resources, which are architecturally very different from the classical control system model. In ANNEX VI an overview of the requirements for the protocols are given based on the Foundational Requirements FR1-7) framework. Regardless of FR grouping, a protocol should also have:

- Secure key management model: rotation, expiry, rekey, revocation, and algorithm agility.
- Cryptographic agility & versioning: explicit protocol versions; clean deprecation path; no silent downgrade.
- Secure defaults & hardening options: insecure modes off by default; minimal optional legacy features.
- Interoperable identity formats: stable identifiers for devices/services; support for certificate identity mapping.
- Segregation of duties: separate admin/config operations from control operations (or make them independently authorizable).
- Formal threat model & testability: clear security claims, negative test cases, fuzzing guidance, and conformance tests.

IEC 62443-3-3 and 62443-4-2 structure detailed requirements under the same FRs, so this checklist is the protocol-level expression hinted by that grouping.

It is important to note that FR requirements are extremely comprehensive, and it is not feasible to design a communication protocol that mitigates all risks identified by the standard. Rather, the list is a set of properties to strive for, and a tool to identify remaining



security risks that can then be mitigated on a different level, such as the security architecture, real-time monitoring, device security and operational processes.

In this, it is also advised to investigate to what extent protocols enable or assist additional security controls. Examples are the data quality flag in 61850, a key management scheme that gives access to monitoring keys to corresponding devices (an interesting example here is the LoRa protocol, which uses different keys for authentication and encryption, allowing to risk the exposure of the encryption key without endangering message integrity), and support for firewall friendly architecture (e.g., through a dedicated port that makes the protocol easy to recognize), or even friendliness to data-diodes.

When looking at gaps, we also need to take into account that not all protocols are attempting to solve all problems. Layer 2 protocols, for example, will usually not attempt to provide user control (who is allowed to perform what switch), while layer 6 protocols don't usually concern themselves with network reliability. Thus, in the end, we may also have a combination of protocols that can fill each other's gaps.

MITRE ATT&CK for ICS lens. In addition to the IEC 62443 foundational requirements, the protocol analysis below can be checked against MITRE ATT&CK for ICS. This adds an attacker-behaviour perspective: rather than asking only whether a protocol provides authentication, integrity, confidentiality or availability support, it asks whether the protocol enables, limits or exposes techniques such as adversary-in-the-middle, automated collection, network sniffing, spoofed reporting messages, unauthorised command messages, alarm suppression, blocking of command or reporting messages, denial of service, loss of view, loss of control and manipulation of control. This lens highlights several gaps that are not always visible from a purely standards-compliance perspective, engineering access, and abuse by authenticated but compromised devices.

5.2.2.2 Relevant OT Communication Protocols

In this section we show the results of three communication protocols: Modbus, IEC 61850 and IEC 62351. Using the same approach we have analyzed Deterministic Ethernet, CAN bus, 450 Connect, DNP3, IEC 60870-5-104 (often shortened to IEC 104), Constrained Application Protocol (CoAP), Device Language Message Specification (DLMS), Meter-BUS (often shortened to Mbus), Message Queuing Telemetry Transport (MQTT), three Narrowband Power Line Communications (NB-PLC): Meters and More, G3 PLC and PRIME and the Open Platform Communications Unified Architecture (OPC-UA). For results in the same format as below see ANNEX V where other communication protocols considered in this assignment are compared against the Foundational Requirements (FR1-7). For an explanation of the FR1-7 refer to ANNEX VI.

Modbus. This protocol is one of the oldest and most widely adopted industrial communication protocols, originally developed by Modicon (now Schneider Electric) in 1979 for use with programmable logic controllers (PLCs). Its longevity and popularity stem from its simplicity, openness, and ease of implementation, making it a de facto standard across manufacturing, energy (down to modern DER setups), building automation, and process industries. Modbus defines a simple request-response communication model in which a client initiates queries and a server.



Pure Modbus offers no security whatsoever and is thus open to attack from anyone inside the network; the little defense it has is obscurity, as it has no concept of data-models as newer protocols do. Proprietary higher-level protocols (e.g., Schneider Unity) for device management often have additional security measures.

Modbus Secure is an extension of the traditional Modbus protocol that adds cybersecurity features to address the lack of native protection in Modbus RTU and Modbus TCP. Defined by the Modbus Organization, it uses Transport Layer Security (TLS) over TCP/IP to provide authentication, data encryption, and message integrity. It is practically not found in the wild.

The most interesting gap is usability; Modbus Secure was specified in 2018 and is essentially not used or offered by manufacturers yet. It thus serves as a good case study on technical measures not being enough for security if they pose a hurdle to integration.

Modbus in the IEC 62443 Structure. Modbus is a straightforward client/server protocol originally designed for serial links and later adapted to TCP/IP (Modbus TCP). Its main design goals were simplicity, deterministic behavior, and a vendor-neutral standard, but the original standard does not feature any security. There are security features built into proprietary add-ons, such as Schneider Unity, but they do not affect the core communication protocol.

Nevertheless, Modbus does have some accidental security features. The use of a dedicated IP port (port 502) makes it rather firewall-friendly and allows to configure a firewall to allow only Modbus traffic. Its relative simplicity does allow for simple, and thus less error-prone, implementations (which unfortunately does not mean there are no Modbus devices with a buffer overflow). The simple client-server architecture also makes it relatively hard to abuse Modbus devices to help in a denial-of-service attack.

Modbus Secure does add more security (i.e., TLS encryption) but has found an extremely low adoption rate since its definition in 2018; it is thus a great study case on why secure protocols are not used even if they are available unless it becomes a regulatory requirement. TLS itself is a good choice as it provides well-understood security functionality and allows on-the-fly updates of the security protocols; the price is a somewhat higher complexity, which contrasts to the simplicity of Modbus itself.

Modbus (with TLS 1.2) mandates as a minimum to support TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. TLS 1.3 is recommended in the newer versions, but not mandatory.

Modbus Summary. Listing the gaps of plain Modbus is pointless, as the protocol has no security measures whatsoever; all the security measures have to come from the outside. This puts high requirements to the surrounding security architecture and thus requires either additional hardware or very strict physical security, i.e., security gateways, strict zoning, one-way or filtered access (data-diodes or protocol aware firewalls), RBAC on the level of HMI or gateways, monitoring, and risk-acceptance with the corresponding procedures. The comparison against FR1-7 is presented in Table 5-3.

Modbus Secure fares somewhat better but also leaves wide gaps; its strongest feature is integrity protection, which is not always the most relevant property in a control system setting and may be detrimental to monitoring solutions.



In terms of mitigation, it appears that even the moderate security level offered by Modbus Secure by modern standards is not gaining much traction, thus adding more technical measures will likely face the same issue. This gap needs to be fixed outside of the protocol standard itself, by providing the appropriate tooling to be able to install and operate a secure version of the protocol, regulatory pressure, architectural isolation of Modbus devices, and potentially avoiding the use of the standard at all in favor of standards with a more integrated security concept.

Table 5-3. Foundational Requirements FR1-7 - Modbus assessment.

Foundational Requirement	Modbus assessment
FR1: Identification and Authentication	Weak for plain Modbus: the base protocol provides no device, user, or message-level authentication. Modbus Secure can provide certificate-based endpoint authentication through TLS, but this does not by itself create a rich protocol-native user identity model.
FR2: Use Control	Weak. Plain Modbus has no concept of users, roles, permissions, or command-level authorization; any host that can connect can attempt read or write operations. Modbus Secure can support stronger client identity and may support role-related certificate attributes but detailed least-privilege enforcement normally has to be implemented in gateways, HMIs, PLC configuration, or surrounding control systems.
FR3: System Integrity	Weak for plain Modbus: commands and responses can be modified, spoofed, or replayed by an attacker with network access. Modbus Secure improves transport integrity and replay protection through TLS, but it does not prevent misuse by an authenticated or compromised endpoint that is authorised to communicate.
FR4: Data Confidentiality	Weak for plain Modbus because all traffic is sent in cleartext. Modbus Secure provides confidentiality through TLS, but encrypted traffic can reduce passive monitoring and troubleshooting visibility unless monitoring, key management, and inspection approaches are designed deliberately.
FR5: Restricted Data Flow	Moderate at the architectural level. Modbus uses simple client-server communication and well-known ports, which makes it relatively firewall-friendly and suitable for zoning, conduits, allow-listing, and protocol-aware gateways. The protocol itself is not zone-aware and does not separate operational traffic from engineering or administrative functions.
FR6: Timely Response to Events	Weak. Modbus does not define security event semantics, audit trails, command accountability, or logging for authentication failures and policy violations. Detection and response therefore depend on PLC logs, gateways, network monitoring, IDS, SIEM integration, and operational procedures.
FR7: Resource Availability	Limited to moderate. The simplicity of Modbus reduces implementation complexity and limits some amplification risks, but the protocol has no native rate limiting, priority handling, connection control, or DoS protection. Availability must be protected through segmentation, strict allow-listing, rate limiting, protocol-aware firewalls, monitoring, and safe fallback procedures.



IEC 61850. IEC 61850 is an international standard for communication networks and systems in electrical substations that defines a comprehensive, object-oriented data model and a set of services for protection, control, monitoring, and automation. It enables high-speed, interoperable communication between intelligent electronic devices (IEDs) using Ethernet-based networks, with protocols such as MMS for client-server communication and GOOSE and Sampled Values for time-critical messaging. By standardizing both the meaning of data and how it is exchanged, IEC 61850 reduces engineering effort, supports device interoperability from different vendors, and facilitates flexible, scalable, and future-proof substation and power system automation. IEC 61850 has a Data Quality Bit included, which is very beneficial for the power system. The standard could improve by including a Recommended Configuration. The comparison against FR1-7 is presented in Table 5-4.

Table 5-4. Foundational Requirements FR1-7 – IEC 61850.

Foundational Requirement	IEC 61850
FR1: Identification and Authentication	Moderate to good when IEC 62351 is applied. MMS communication can use certificate-based authentication and TLS profiles; GOOSE and Sampled Values require IEC 62351-6 mechanisms or architectural controls because the base multicast services do not provide authentication by default.
FR2: Use Control	Moderate. IEC 61850 has a rich object model and access control can be supported through IEC 62351-8 role-based access control, but practical enforcement depends on IED configuration, engineering tools, and operational governance.
FR3: System Integrity	Mixed. MMS can be protected using IEC 62351 profiles, while GOOSE and Sampled Values require special treatment because of their low-latency multicast nature. Without IEC 62351-6 or equivalent controls, spoofing and modification risks remain.
FR4: Data Confidentiality	Good for MMS when TLS is enabled. Confidentiality for GOOSE and Sampled Values is more constrained by latency and multicast operation and is often handled by zoning, MACsec, or other network-layer protection rather than by the base protocol.
FR5: Restricted Data Flow	Good architectural support. IEC 61850 engineering, SCL configuration, logical nodes, VLANs, and service separation support precise network design, but multicast traffic and engineering access still require careful zoning and filtering.
FR6: Timely Response to Events	Good for operational events: GOOSE, Sampled Values, reports, logs, quality flags, and time synchronization support fast protection and monitoring. Security event semantics and SOC integration remain dependent on IEC 62351, device capabilities, and operator tooling.



Foundational Requirement	IEC 61850
FR7: Resource Availability	Good when engineered with redundancy and traffic engineering, but sensitive to multicast storms, malformed requests, time-sync attacks, and high-load services. Availability depends strongly on network design, redundancy, rate limiting, and hardening.

IEC 62351. This series of international standards defines cybersecurity measures for power system communication protocols used in substation and grid automation. It specifies methods for authentication, encryption, data integrity, role-based access control, and secure key management to protect protocols such as IEC 61850, IEC 60870-5-104, DNP3. IEC 62351 is aimed at enabling interoperability and selecting standards that preserve the reliability and real-time requirements of critical power system operations. IEC 62351 does not define the technologies itself but rather serves as a bridge to select the appropriate technical standards, e.g., NIST standards for encryption. The comparison against FR 1-7 is presented in Table 5-5.

The “original sin” of IEC 62351 was that the standard did not enforce an upgrade path for its security primitives and thus has to support legacy protocols that should not be used anymore in modern systems. Though IEC 62351 is evolving and newer versions are including newer primitives, it still allows outdated mechanisms such as TLS 1.2 rather than TLS 1.3, non-agile protocols and comparatively weak configurations. While that makes it easier to integrate legacy systems, it also makes it substantially harder to adapt to modern requirements and security over the expected lifecycle of a device, such as the need for post-quantum migration. Another gap worth discussing is the use of slow protocols such as RSA 4096 for the extremely real-time-critical GOOSE protocol; modern signature schemes such as Ed25519 might have been a much better choice here.

Table 5-5. Foundational Requirements FR1-7 – IEC 62351.

Foundational Requirement	IEC 62351
FR1: Identification and Authentication	Good as a security companion standard: IEC 62351 profiles certificate-based authentication, TLS, application-layer authentication, and role-aware identities for several IEC TC57 protocols.
FR2: Use Control	Good in principle through IEC 62351-8 role-based access control and role-to-permission mappings. Practical effectiveness depends on consistent implementation, provisioning, and integration with operational identity management.
FR3: System Integrity	Good. IEC 62351 provides profiles for message authentication, integrity protection, replay protection, digital signatures, and secure profiles for MMS, IEC 60870-5, DNP3, GOOSE, and Sampled Values.



Foundational Requirement	IEC 62351
FR4: Data Confidentiality	Good where TLS or encryption profiles are applicable. Confidentiality is more difficult for low-latency multicast services and legacy deployments and may require selective protection or supporting network controls.
FR5: Restricted Data Flow	Moderate. IEC 62351 supports secure profiles and role separation but does not by itself create zones and conduits; segmentation, routing, firewalling, and data-diode concepts remain architectural responsibilities.
FR6: Timely Response to Events	Moderate to good. IEC 62351 includes security event and network management concepts, but consistent logging, alerting, and SOC integration depend on product support and operational deployment.
FR7: Resource Availability	Moderate. IEC 62351 improves resilience against spoofing, replay, and unauthorised commands, but cryptographic overhead, certificate handling, and legacy compatibility can affect availability if not engineered carefully.

5.2.3 Technical standards

Device-level and technical standards address the mechanisms that enable secure implementation of communication, control, and protection functions. Unlike framework standards, which define governance structures and security objectives, technical standards specify concrete building blocks such as cryptographic algorithms, secure communication profiles, random-number generation, key-management requirements, device hardening, and robustness properties. For the purpose of this document, we differ between communication standards (which are often highly adapted to the OT world) and other technical standards that provide generic building blocks such as device security or encryption.

For OT environments, these standards are important because many security properties depend not only on network architecture or organizational controls, but also on the capabilities of individual devices. Field devices, controllers, gateways, meters, IEDs, and communication modules must be able to authenticate peers, protect message integrity, support secure configuration, resist malformed inputs, and remain available under adverse operational conditions. However, technical standards are often generic and not designed specifically for long-lived, resource-constrained, real-time OT environments. This creates practical gaps when technically sound mechanisms are difficult to deploy, maintain, update, or monitor in operational systems.

The following subsections therefore summarize relevant technical building blocks and identify where additional OT-specific guidance is required.

Cryptographic Primitives. A core requirement for secure communication protocols is the protection of confidentiality, integrity, and authenticity. In OT environments, confidentiality is not always the dominant requirement, but integrity and authenticity are usually essential: devices and operators must be able to trust that a message originates from the claimed sender and has not been modified in transit.



These properties are normally achieved through cryptographic mechanisms. In some OT settings, physical protection of cables and equipment can reduce exposure, but physical protection alone is no longer sufficient for modern, distributed and increasingly connected grid environments. Cryptographic protection is therefore a necessary technical foundation, even if it must be balanced against latency, resource constraints, maintainability, and safety requirements.

These properties are usually enforced through cryptographic means (there are some cases in OT systems where access to a physical cable is restricted and controlled).

Symmetric Cryptography assumes both sides of the communication have a shared secret key, which can then be used to establish confidentiality (through encryption) and integrity/authenticity (through message authentication). The corresponding algorithms are well understood and performant; the main challenge in the deployment is to establish and maintain the shared secret inside a complex and dynamic system.

AES (FIPS PUB 197 / ISO-IEC 18033-3) is the primary standard used for encryption. It comes in two variants with different key sizes (128 to 256 bit) and encrypts messages as blocks. To be fully functional, AES needs to be accompanied by a mode of operation. This can add uniqueness to the encryption (so that the same plaintext block does not always encrypt into the same ciphertext) but can also add authentication. Commonly used modes of operation are Galois-Counter Mode (GCM), CCM, and CCM*

NIST SP 800-38A (Modes of operation for Confidentiality), Authentication Only (SP 800-38B), SP 800-38C (CCM), D (GCM, GMAC), IEEE 802.15.4, Annex B

AES is quite resilient against quantum computers, as the best-known quantum algorithm (Grover's Algorithm) only provides a quadratic speedup, and thus – in the worst case – halves the effective key length. To be on the safe side, the key length should thus be set to 256 bit.

Asymmetric Cryptography does not require a shared key and thus offers substantially more flexibility at the price of less efficiency and longer key size. It can be used to establish a shared key between two parties without an interloper learning that key, digitally signing messages in a way that they are publicly verifiable, as well as advanced use cases such as performing entire computations on encrypted data.

Classical asymmetric encryption is vulnerable to quantum computers and is thus recommended to be phased out. To this end, NIST has standardized new algorithms (ML-KEM for key exchange, ML-DSA and SLH-DSA for digital signatures). Those do come with longer key sizes and less practical experience.

Transport Layer Security (TLS). Usually, a combination of symmetric and asymmetric cryptography is used. A digital signature with a corresponding certificate is used to authenticate an identity, and using this, a key-agreement protocol is used to establish a shared key that can then be used with symmetric cryptography. An example of this is TLS, a standard used for internet encryption. The configuration, or crypto-suite, then looks like this: *TLS_KeyExchange_Authentication_Encryption_Integrity*.

This means TLS using Elliptic-Curve Diffie-Hellman for key exchange, RSA for authentication, AES-128 with Cipher Block Chaining for encryption, and the SHA-256 hash function for message integrity. In negotiating the crypto-suites in a handshake



during the initialization of communication, TLS allows for protocol agility, i.e., the cryptographic protocols can be changed on a live system; to this end, new cipher suites can be added to different devices over time, and newer ones can be used once available on both communicating devices, slowly phasing out the old ones.

In TLS 1.3, the Cipher suite only defines the symmetric encryption and the hash function (e.g., TLS_AES_128_GCM_SHA256), where the symmetric cipher has to provide an authenticated encryption (AEAD, authenticated encryption with associated data – the latter is additional data that is only authenticated, e.g., for routing information). Key exchange and Signature algorithm are still negotiated, but separately – this sounds more complicated, but allows for some more simplicity, as a computer does not need to announce the support of every combination of key exchange and symmetric cipher. If anywhere possible, TLS 1.2 should be retired and replaced by the more modern version, especially in light of post-quantum cryptography.

An example for non-standard cryptography and the fragility against wrong use is the OSGP protocol, which combined the RC4 cipher with a self-made authentication function; this combination allowed an attacker to test individual key bits, and thus recover the authentication and encryption key by sending about 50 messages to a device and watching its response. It is vital to use cryptography in a way that has been standardized or perform an expert analysis and public review of changes if they are necessary (as done, for example, by 801.15.4 with CCM*). For completely new algorithms (such as the post quantum ones), the normal procedure is that a standard body (usually NIST) organizes a public competition, and over the next years the entire community analyses each other's approaches to determine the eventual winner – an effort that goes far beyond what any individual company can deliver.

Cryptographic Keys Properties. One common mistake is the use of poorly generated or reused random numbers; this has led to successful attacks, for example on the Sony PlayStation copyright protection scheme. To assist with this topic, there are standards for generating and testing random numbers, such as BSI AIS 20 and AIS 31, as well as frequently updated recommendations on key length depending on the anticipated system lifetime, including FIPS 186-5, 56A, 203, 204, 205, 800-13 and BSI TR 02102-1 Version 2.

Robustness Standards. OT devices have a long tradition of environmental robustness, e.g., IEEE 1613, which defines how devices handle rough environments. Other standards such as IEC 61508, and to some extent IEC 61511, drive safety-relevant behaviour, e.g., devices detecting a failure and rapidly restarting. These standards look at systems from a safety point of view and thus lack a security point of view. On the security side, a number of standards such as FIPS 140-3 have defined secure devices, but do not scale well to large-scale usage of OT devices and are barely used there. One exception is the German Smart Meter Gateway, which is required to satisfy high security standards, but consequently was a major problem for vendors to implement.

IEC 62443-4-2 does cover robustness through Foundational Requirement 7 (Resource Availability) but defines requirements rather than giving guidance. IEC 62443-4-1 gives some guidance on good engineering, but the convergence of good and practical secure implementation standards and OT requirements is a process that is still ongoing and currently can still be considered lacking.



With increasing IT/OT convergence, some IT technologies, such as the use of Trusted Platform Modules (TPMs), are slowly entering the OT domain. This is promising for security but could also benefit from more structural guidance through standards.

5.2.4 Synthesized requirements

This section analyzes common security standards used in the Power and related OT sectors for gaps that are inherent to the standards, originate from standards not fully fitting their use cases, or new risks coming up that the standards cannot fully cover yet¹. In this, four groups are identified and in addition, some background sections relevant for understanding the gaps is provided, (e.g. basic functioning of cryptography):

- Generic gaps are gaps that are common to many standards and thus pointing them out for each individual standard would be redundant. This mainly covers issues that are generally difficult to standardize, and issues that came up due to recent developments that the standardization world did not react to at this point
- Security Frameworks such as ISO 2700x and IEC 62443 are used by organizations to structure and organize their security and can usually be certified against. Gaps in those standards are particularly relevant, as they can have an amplified effect, and many organizations primarily aim for standards compliance.

In addition to being the target of the gap analysis, these standards also can give a checklist of properties expected from the more technical standards, and in this also assist as a reference for the gap analysis of those.

- Communication standards form the backbone of IT and OT networks, and gaps therein can easily become critical if not mitigated.
- Further technical standards can cover device security, access control, and similar issues. There are comparatively few of those in the OT arena, but those should be addressed as well.

5.2.4.1 Cross Standard Gaps and Recommendations

Some gaps may affect more than one standard, either because the issues are generally hard to address in a standard, or because the issues are comparatively new and have not yet been addressed by standards work. These gaps are not necessarily IEC 62443-related but may also cover gaps where IEC 62443 has a blind spot or has not yet been adapted to new developments and requirements.

Quantum Readiness. Quantum computers, once available, have the problematic property of being able to break all commonly used public key protocols, and thus affect digital certificates, key agreement schemes, and many more. According to NIST, there

¹ Note to the reader: The identified gaps are relevant for stakeholders in the EPES like standard bodies, suppliers and network operators. Each stakeholder needs to assess urgency, impact, implementation relevance and timing for its own organization.



now is a 2030 deadline to deprecate all classic public key protocols, and 2035 to have completely mitigated them. Replacement algorithms do exist now, but none of them have been taken into account by OT standards at this point; their integration is also non-trivial, as they do tend to impose more requirements on available resources.

Recommendation: It is vital to provide protocol agility (see below), to be able to change protocols on the fly without having to update the entire system all at once. Also, one part that is usually out of scope for most standards, devices and network capacity should have sufficient spare resources to fit in with the new protocols.

The higher-level standards should assist with an approach to quantum risk assessment and explore mitigations of quantum risks if protocol replacement is infeasible, for example due to hardware constraints, missing vendor support, or the logistics of updating a cryptographic primitive in a complex live system.

Special care needs to be taken for hidden dependencies – unsafe cryptography may be hidden in easy to overlook services (such as time synchronization), post quantum protocols may change communication and memory performance, and devices may have hardware crypto accelerators that will not support the new protocols anymore.

Physical Security. There are numerous physical security standards, most of which are out of scope here, even though they also now have large gaps due to hybrid warfare with drones, violence-as-a-service, etc. What is interesting for our scope is the intersection between cyber and physical security. This is especially relevant for the power grid, as many generic security standards assume that all hardware is in a physically well-secured environment, which is not possible to assure for thousands of substations. The risk there is increasing not only due to the changing geopolitical landscape, but also due to the increasing distribution of connected, and in large numbers critical, grid resources through small renewables or even smart meters.

Recommendations: It is out of scope for most standards discussed here to address physical security directly. However, standards can drop the assumption of physically untouchable networks and apply a more Zero-Trust-oriented approach, i.e., no device, network or zone is trusted per se. Standards might also highlight devices that have to be trusted and thus mark them as requiring a higher level of tamper resistance or physical security.

Another aspect that is out of scope for most standards is backdoor freeness. Many devices have deliberately built-in capabilities for a physically present agent to gain root access, which eases maintenance, but relies on an assumption that is increasingly difficult to justify.

Key Management. Many communication standards lack on the key management side; this is a major reason security measures are not implemented, or fall back to trivial solutions (e.g., both in Spain and the UK all smart meters had the same key; the same holds for some DSO's substation automation. Key management in OT scenarios does have additional challenges as it has to be highly reliable – if a device misses a key-update and then cannot react to commands anymore, there can be massive safety implications. It is also harder to execute if devices are physically spread, asset management is incomplete, and some devices are not always on.



Recommendation: Key management is a difficult, but also well researched problem. If a standard can define the exact requirements and identify where compromises are possible, there usually is some way to implement a key management system that fits into the gap (see as an example the ZigBee healthcare key management, which utilizes the fact that the number of involved devices is comparatively low and missing devices will be identified reasonably quickly to implement a high-speed key agreement for low power devices).

Complexity / Integrability. Another reason security measures are not integrated is that the OT systems are difficult enough to implement and interoperate as-is, and security is adding new points of failure and interoperability challenges. In practice, this is one of the reasons why many communication protocols forego all security.

Recommendation: This is the most difficult problem to address, as this is where security requirements collide with operational practices, and many of the OT systems used are designed in a sufficiently fragile way that keeping them running in the first place is a major endeavor. It would be an interesting follow-on research project to work with integrators and system engineers to distill their requirements for a maintainable system and develop approaches to integrate those with a valid security architecture, as well as collecting best practices from the operators who manage.

Monitoring & IDS (Intrusion Detection System) Capabilities. Given the difficulty of securing systems, it is vital to allow for efficient monitoring. While the monitoring systems themselves are out of scope, standards should make sure to provide the relevant access, store the relevant information, and in general keep in mind that it has to be possible to perform meaningful security monitoring.

Recommendation: A useful mitigation of this issue is demonstrated in the LoRa protocol. This protocol uses different keys for authentication and encryption. This allows an IDS to be given the decryption key, while preserving full end-to-end security for the authentication keys. Unfortunately, this approach has not yet been integrated into a NIST-standardized mode of operation.

Maintenance Backdoors. Many Systems in the wild have undocumented maintenance backdoors, which do pose a security risk. This points to two gaps – regular maintenance (or failure recovery) is insufficient, and there is a lack of negative requirements (i.e., forbidding undocumented functionality)

Protocol Agility. In security, protocols age; algorithms that used to be considered secure, such as DES, RC4 and SHA-1, are eventually deprecated. If they are hard coded without the possibility to switch algorithms on a live system, as TLS does this fairly well, outdated protocols stick around well past their due date.

Recommendation: TLS demonstrates well how this can be implemented. At the beginning of each communication, the handshake, both sides negotiate supported protocols and then agree on the best one both sides can handle, whereas devices can refuse to communicate with outdated protocols. This allows new protocols to be implemented piece by piece and lets devices switch to them once all partners support the newer version. There is still some work in asset management to ensure all devices are updated, so that an old protocol can eventually be retired for good.



Cloud Integration & Mass deployment. A large part of grid functionality is slowly migrating to cloud providers; this requires new standard properties, as most standards assume that everything is on site. It also creates new single points of failure, where independent systems can suddenly be hosted in the same cloud, as well as interactions such as a power outage affecting server farms, which then feeds back into grid operations.

Another often neglected factor is the mass deployment of usually uncritical devices; balcony PV generation in Germany now is a significant factor in grid stability, and thus a substantial risk. This also requires additional coordination (as a non-security example – PVs should now all shut down when they measure a specific undervoltage, but add some randomization to the parameters to smoothen out the process

Robustness requirements. Many standards define what is supposed to happen but lack a definition of what happens if something goes wrong, e.g., a malformed message might still be processed and thus lead to an undefined state.

5.2.4.2 IEC 62443 Gaps and Recommendations

Implementability. One of the primary shortcomings of security mechanisms in the field appears to be practical usability. In the example of Modbus, the security extension Secure Modbus was published in 2018, yet the authors are not aware of any serious usage of that variation. This cannot be explained through resource constraints or implementation issues on the device side; modern PLCs and Ethernet networks have sufficient spare resources to support the security extension.

We suspect that the primary reason for non-adoption is the additional integration effort required to integrate, test and monitor a network with built-in security, in addition to the added risks of errors in key management that can lead to system malfunction.

It is out of scope for this document to solve the problem of integration and potential safety/security conflicts, but some approach would merit further investigation:

Debug modes. One idea that is to some extent implemented in 61850 is a debug flag – some operations that are necessary for debugging but pose a security risk are marked with the debug-flag, so the receiver of the corresponding messages can react accordingly. In 61850, this is used for example if a PLC sends forced outputs (i.e., sends output values that are set directly rather than representing any state). A debug mode for authentication could send un/wrongly authenticate messages for testing purposes but would make it transparent to all receivers of such messages that this is now happening.

Authentication only. Even though confidentiality is a primary concern of information security, it is a less critical property for OT networks. While it is still advantageous to have it, e.g., to prevent an attacker from learning about the system layout by simply observing, it also poses problems for monitoring and debugging and does not allow for an easy fallback for devices that do not possess the current encryption key. A solution would be to use different keys for encryption and authentication: encryption being done with a static, network-wide key to provide some protection with no constraints on operation, while authentication is done in a more secure way with individualized keys.



Robust key management with safe rollover. It is well possible in a large OT system that some devices miss a key update and thus authenticate messages with an old key. The safety risks of that can be mitigated by receiving devices still accepting outdated keys (which adds some risk but is still better than not requiring a key at all) but immediately raise an alert. This allows to either detect the late devices and perform a key update, immediately detect an attack that is using an old key, or to add an exemption for devices that for some reason cannot receive an updated key.

Advanced Key Management Solutions. Key management – i.e., providing shared keys for symmetric cryptography – is a major problem for most complex systems. If keys need to occasionally change for security reasons. If the system and its requirements are well understood, however, it is usually possible to provide a key management scheme that provides a solution that mitigates most of the pain in maintaining these keys. In the ZigBee Key Management for Medical Devices profile, for example, the special setting - a limited number of physically somewhat protected devices with centralized commissioning – is used to derive a special key derivation scheme that allows each pair of devices to efficiently compute their own shared key, which massively reduced the risk of key leakage. Similarly, a standard can offer a library of commissioning and key update schemes which can then be used to optimally adapt to the given use case and settings the system is in. Mal-authentication should lead to alarms rather than immediate discarding of the message.

Trust flags. An approach that is (to some extend) done in 61850, measurement values can have different trust levels – thus, an unauthenticated message (or one with an old key) would be treated as less trusted, rather than immediately discarded.

Asset Ownership. As an industrial control system standard, the physical model for IEC 62443 is a set of industrial sites, which are mostly physically secured. This model does not reflect the reality of the electricity system. Due to its geographic reach, it has always been widely geographically distributed, with endpoints that are difficult to physically secure. In recent years, through the massive increase of distributed energy resources (DER) and car charging systems, this spread has gone even further, and it has become vital to also extend the control systems to the many distributed systems. This has added the challenge of asset ownership, as these plants are not owned by the network provider, and in many cases by private individuals with little regulatory oversight. Furthermore, the increased requirement for IT components is motivating a number of network providers as well as owners of DER to adopt cloud solutions, which also means that some critical components are on remote servers, and we get a new set of unknown and hard-to-control dependencies.

Physical Security. Similar to the point above, the traditional model assumes that most devices can be implemented in a reasonably secure physical environment, making it hard for an attacker to obtain direct network or device access. This assumption is difficult to maintain in the electricity grid setting, and more IT components are moving away from protected data centers to the edges of the grid. Furthermore, geopolitical changes have decreased the effort required to perform a physical intrusion. For physical attacks, the concept of “violence as a service” has been established in recent years, allowing attackers to cheaply and anonymously hire throw-away assets through Telegram and



similar channels. Using such assets for cyber-physical attacks is straightforward and, though less visible in the news, likely commonplace already.

Real time requirements. As 2700x, the 62443 standard recommends mitigating existing risks by adding more security controls. This can be counterproductive in a system where real-time constraints and safety functionality are critical – an additional firewall can be both a safety risk and a danger to real-time communication and extremely time sensitive systems – such as protection switches – can barely afford the time for extensive cryptography

Operational IT. The integration of IT and OT is an ever-changing topic, and standards have a hard time keeping up with the new reality. While IT and OT were initially neatly separated, we now not only see communication lines between the two worlds, but also IT components entering the OT domain, e.g., PLCs that are entirely based on a variation of Linux. This setting keeps rewriting the rules: if IT components are present in OT devices, they also inherit many vulnerabilities, and an OT patching strategy as proposed in IEC 62443 may not be sufficient anymore.

Monitoring and Forensics Support. Though FR6 covers timely reaction to events, monitoring issues should be highlighted more. The lack of personnel to perform OT monitoring combined with the inability to outsource OT monitoring to an external IT SOC is a problem that haunts many operators. Protocols that are designed for extensive logging and enforce the data richness that make it easier to detect an anomaly can be of great assistance here. One special aspect of this is proactive forensics. As shown by many past incidents, with Triton as a prime example, the threat model for the electricity grid is not the same as for most commercial settings. Many potential attackers, including those with whom one might have a friendly relationship now, do not wait for a conflict to arise to start their attacks, but rather attempt to compromise a system well in advance in case this is needed at some point. There are ways to design systems so that some form of proactive forensics is built in, i.e., hooks in the system that assists an analysis of a live system for potential compromises.

Artificial Intelligence (AI). For obvious reasons, the current security frameworks cannot take into account recent developments in artificial intelligence. While there is no direct impact at this point, though operators are now considering the use of AI in future settings, there are some indirect consequences. On the negative side, AI can and already does automate some attacks, allowing lower-level attackers to reach beyond their normal capabilities. Lower-level attackers can perform as efficiently as higher-level attackers and thus target more systems and analyze targeted systems faster and more thoroughly. Also, AI-based analysis and programming massively speed up the development of exploit software and bug finding; within ten years, the average time from known vulnerability to working exploit code has decreased from more than two years to hours, which massively upsets OT-specific issues such as performing a risk analysis for every patch. If the OT system has an internal AI, this could also be abused to guide an attack from the inside, thus allowing malware that cannot easily communicate with the outside world to act in a more competent autonomous way; Stuxnet is an example where malware that was forced to act independently ultimately was detected due to misjudgments.



On the defender side, AI can process substantially more monitoring data, which would allow for more data-rich monitoring information added to the protocols that then allow for a more effective SIEM.

Modern Best Practices. Over the last years, innovative grid operators have added technologies and approaches that go beyond what standards prescribe, and for which consequently little guidance exists. An example is the ability to go into full island mode, i.e., to disconnect and later reconnect the entire OT operation from any public network without causing significant business interruption, as long as the disconnection is temporary. This allows operators to enter a secure mode based on a small suspicion of a problem, thereby increasing reaction time while buying time to analyze the issue.

5.2.5 KERs that support the framework standard IEC 62443

This section evaluates the contribution of the eFORT KERs to the implementation of IEC 62443 (see Table 5-6 for the results). It identifies the KERs that support the requirements and security objectives of the standard, highlighting how the project outcomes can facilitate the adoption of cybersecurity best practices in operational technology (OT) environments.

5.2.5.1 eFORT Intelligent Platform (KER 1)

IEC 62443 defines required security functions but does not prescribe an integrated operational platform combining monitoring, visualization and response. The platform can support IEC 62443-3-3 system security requirements for monitoring, detection and event handling, and IEC 62443-3-2 risk-based system architecture. It can provide an integrated operational platform enabling coordinated, real-time cyber-physical situational awareness and response.

Table 5-6. KERs supporting IEC 62443

KER	KER name	Support to IEC 62443
1	eFORT Intelligent Platform	IEC 62443-3-2 & IEC 62443-3-3
2	Data Base Tool	IEC 62443-2-1 & IEC 62443-3-2
3	Secure Box	IEC 62443-3-3 & IEC 62443-4-2
4	Training through CRoF and digital twin of the power grids	IEC 62443-2-1 & IEC 62443-3-2
8	IDS	IEC 62443-3-3
9	SIEM	IEC 62443-2-1 & IEC 62443-3-3



KER	KER name	Support to IEC 62443
10	ChatBot	IEC 62443-2-1
12	RTU	IEC 62443-4-2.
13	Blockchain for grid resiliency	IEC 62443-3-3
14	SOAR	IEC 62443-2-1 & IEC 62443-3-3
15	Blueprint for EPES SOC infrastructure	IEC 62443-2-1
21	Connected devices vulnerabilities	IEC 62443-2-3 & IEC 62443-3-2

5.2.5.2 Data Base Tool (KER 2)

IEC 62443 requires risk and vulnerability management but does not define tools for continuous visualization or monitoring. The tool aligns with IEC 62443-3-2 requirements for asset identification, vulnerability identification and risk assessment, and IEC 62443-2-1 security management processes. It can add real-time, combined static and dynamic vulnerability visualization beyond document-based risk assessments.

5.2.5.3 Secure Box (KER 3)

IEC 62443 specifies technical security requirements but does not define concrete deployable protection devices. The Secure Box maps to IEC 62443-4-2 component security requirements and IEC 62443-3-3 boundary protection and integrity requirements. It can provide a ready to deploy cyber physical protection device tailored for substation and microgrid environments.

5.2.5.4 CRoF training and digital twin environment (KER 4)

IEC 62443 requires training and awareness but does not specify training methods or simulation environments. It can support IEC 62443-2-1 requirements for competence, training and awareness, and IEC 62443-3-2 risk understanding. It introduces cyber-physical digital-twin-based training enabling realistic attack simulation and impact assessment.

5.2.5.5 IDS (KER 8)

IEC 62443 requires detection capabilities but does not prescribe detection techniques or intelligence levels. The IDS can support IEC 62443-3-3 requirements for detection of security events and system integrity monitoring. It can add adaptive, AI-based intrusion detection improving responsiveness to evolving threats.



5.2.5.6 SIEM (KER 9)

IEC 62443 mandates monitoring but does not require centralized SIEM solutions. KER 9 can support IEC 62443-3-3 monitoring and IEC 62443-2-1 security operations and incident management. It can enable cross-system log correlation and centralized situational awareness, exceeding baseline monitoring requirements.

5.2.5.7 ChatBot (KER 10)

IEC 62443 does not address operator interaction tools for security operations. the ChatBot can indirectly support IEC 62443-2-1 operational processes and incident response support. It could improve human-machine interaction and operator decision-making during security monitoring and incidents.

5.2.5.8 RTU (KER 12)

IEC 62443 defines security requirements but does not address legacy RTU enhancement. The RTU maps to IEC 62443-4-2 component security requirements for field and control devices. It can facilitate practical IEC 62443 compliance in brownfield installations by enhancing existing RTUs.

5.2.5.9 Blockchain for grid resiliency (KER 13)

IEC 62443 does not reference blockchain or distributed ledger technologies. KER 13 can support integrity and availability objectives in IEC 62443-3-3. It can contribute to introduce supply-chain traceability and cross-TSO monitoring addressing emerging resilience challenges.

5.2.5.10 SOAR (KER 14)

IEC 62443 requires response capabilities but not automated orchestration. SOAR can support IEC 62443-2-1 incident response processes and IEC 62443-3-3 monitoring. It can enable standardized, automated incident response using open standards (e.g. OpenC2, CACAO).

5.2.5.11 Blueprint for EPES SOC infrastructure (KER 15)

IEC 62443 does not define SOC architectures. KER 15 aligns with IEC 62443-2-1 governance and operational organization requirements. It can provide a reusable SOC blueprint accelerating implementation of aligned operations.

5.2.5.12 Connected devices vulnerabilities (KER 21)

IEC 62443 requires vulnerability management but not vulnerability discovery outputs. KER 21 can support IEC 62443-3-2 asset identification and IEC 62443-2-3 vulnerability and patch management. It would help to extends coverage to non-traditional grid devices, supporting broader EPES security.



6 Recommendations and Conclusions

This chapter consolidates the main findings of the eFORT analysis into a set of practical recommendations for improving cybersecurity, resilience, and compliance within future European power systems. The recommendations address both current and emerging challenges associated with the evolving regulatory landscape, the implementation of cybersecurity standards, and the deployment of innovative digital energy solutions. Compliance, certification and training recommendations are addressed at the end of the section.

6.1 Regulations & cost-benefit considerations

Follow best practice even where no obligation applies. The AI Act imposes no cybersecurity duty on KER 1 (eFORT Intelligent Platform) or KER 10 (Chatbot), but that does not mean security controls should be overlooked. Article 95 expressly provides for voluntary application of the high-risk requirements, including the Article 15 cybersecurity requirement, to non-high-risk systems. Under the CRA, a default-category product like KER 12 (RTU) may self-assess with no external verification, but we still recommend independent testing against the Annex I essential requirements.

Be wary of potential costs under the CRA. Since the Annex I of the CRA essential requirements are identical for every in-scope product, the main cost comes from the way manufacturers must prove compliance. The first cost can stem from the conformity route. For KER 8 (IDS) (Class II) and KER 3 (Secure Box) (critical), a notified body is unavoidable under Article 32(3), and third-party verification is a budget line to plan for. More broadly, the vertical standards may impose requirements that current designs do not meet, and retrofitting security properties into hardware such as the Secure Box could be costly. For the Secure Box specifically, critical products are currently assessed under the Class II procedures, but the Commission may, by means of a delegated act, require a European cybersecurity certificate at assurance level at least "substantial" (Art 8(1)), which would raise the cost further.

Monitor the regulations, standards and delegated acts. The relevant regulations are under constant development. Under the CRA, track the harmonised standards under development by CEN-CENELEC and ETSI, since they determine the technical requirements and the delegated acts under Article 8(1) that could make certification mandatory for critical products. The Commission can also amend Annexes III and IV by delegated act, which means that by the time a KER is commercialised, it can be reclassified without the product changing at all. The proposal of the Cybersecurity Act (CSA2, COM(2026) 11 final, 20 January 2026) should be tracked on the same basis. It would task ENISA with running the single-entry point for incident reporting created by the Digital Omnibus, through which one notification could cover obligations currently split across different existing regulations.



6.2 Standards

Introduce quantum readiness for all protocols. Deprecate all classic public key protocols and replace or reinforce them with quantum-ready algorithms. More generally: provide protocol agility and ensure sufficient spare resources to fit in new protocols. TLS demonstrates well how this can be implemented.

Apply zero trust-oriented approaches. Standards for EPES should drop the assumption of physically untouchable networks and secure boundary protection and apply a Zero-Trust-oriented approach. Standards should mark devices that require a higher level of tamper resistance or physical security.

Create explicit maintenance procedures. Standards are explicit in accepting or denying backdoor freeness and make a difference for situations where IT components are present in OT devices and update the OT patching strategy as described in the IEC 62443.

Include usability in the key management requirements. Standards should define the exact requirements and identify where compromises are possible; this allows specialized solutions to be deployed that optimize usability and security in their given context.

Security measure integration. Standards for the EPES should include the impact of cyber security measures on maintenance and operational management and provide best practice examples.

Facilitate the use of intrusion detection systems. Standards should make sure to provide secure access to perform meaningful security monitoring. To facilitate this, standards make a difference between authentication and encryption keys.

Balance positive and negative requirements in standards and procurement. Negative requirements (i.e., forbidding undocumented functionality) get the same amount of attention as positive requirements (required functionality).

Robustness requirements include failure. Standards use equal attention to define what is supposed to happen and what happens if something goes wrong.

Cloud Integration & Mass deployment create new risk factors. EPES cybersecurity standards should include new properties, risk factors, interdependencies and failure modes associated with migrating a large part of grid functionality to cloud providers and edge devices that are not under DSO control.

Explicitly include Artificial Intelligence (AI) into standards. Standards should immediately include the effects of AI in all its breadth, from risk analysis and active attacker use, to use in defensive applications. Given the rapid development and change of AI possibilities, this might require substantially new approaches and different concepts.

Facilitate reactive and proactive monitoring and forensics support. Standards on monitoring should include and enable both reactive and proactive forensic actions.

Perform maintenance according to OT patching strategy. Standards make a difference for situations where IT components are present in OT devices and update the OT patching strategy as described in the IEC 62443.



Real time requirements and cyber security do not always match. Standards allow for alternative cyber security strategies when real time data exchange is essential in EPES operations.

Origin of the assets is an element in the risk analysis. Framework standards relevant for the EPES go beyond the direct ownership and include the risks of massively deployed assets and clouds directly or indirectly connected to the cyber secure system.

6.3 Compliance and certification

Cyber security in the power system is a rapid developing topic. New European regulations like NIS2, NCCS, CRA and country specific rules and regulations are appearing quickly. Put simply, the power sector is facing a rapidly expanding landscape of new regulations, standards, and compliance requirements. The regulations describe what needs to be done (the what), standards say how it can be done (the how). The third and final step is to show that the party (e.g. an OEM, integrator or system operator) complying with the regulations/have followed the appropriate standard (the proof).

This certification (or proof) market is developing in parallel with the new requirements and standards. Since there are many actors in the power system and all components and systems are integrated into one working system, this element is a current hot spot in the market. How to show that you are compliant to all the rules and regulations and follow the correct standards?

For many regulations IEC 62443 is used as the framework standard. Depending on the role in the future power system, companies use the framework standard in a different way. Operators like DSOs and TSOs can use IEC 62443 as the implementation framework for the legal obligation to perform e.g. risk management and implement resilience measures as described in NIS2. Under NIS2, proof of compliance is primarily evidence-based and audit-based, not certificate-based. These audits can be internally or externally, depending on the country. NIS2 expects operational resilience, not point-in-time certification. This includes monitoring, detection and response capabilities, evidence of testing and demonstrated incident handling performance.

For OEM's and system integrators IEC 62443 becomes the technical backbone for compliance. Some regulation directly points towards standards, like the Cyber Resilience Act (CRA), which defines the legal requirement for product cybersecurity certification. CRA is directly linked to IEC 62443 and ENISA introduces EU-wide certification schemes. There are schemes for Component Security Assurance (CSA) certification and IoT Component Security Assurance (ICSA) certification (both based on IEC 62443-4-2), System Security Assurance (SSA) certification (based on IEC 62443-3-3), Security Development Lifecycle Assurance (SDLA) certification (based on IEC 62443-4-1) and finally ACS Security Assurance (ACSSA) certification (based on IEC 62443-2-1, 2-4, 3-2, 3-3). This last certification scheme is very recent (February 2026), showing that the compliance market is moving and tries to keep track of the latest developments.

Certification supports compliance evidence, but it does not automatically prove full regulatory compliance, especially where operational, organizational and system-integration responsibilities remain with the operator. The key market need is therefore



not simply “certification”, but end-to-end compliance assurance. Operators need practical ways to prove that their cybersecurity risk management and operational resilience measures are effective. Manufacturers need to prove that their products are secure by design, securely maintained and supported throughout their lifecycle. Integrators need to demonstrate that products, systems and services are combined in a way that preserves security properties in the actual operating environment. This creates demand for advisory services, gap assessments, testing, audit schemes, documentation, certification support, security engineering, monitoring evidence, training and continuous compliance management.

For EU development projects like eFORT, understanding how compliance is developing is relevant because several project results do contribute to the evidence base required for compliance. Tools and methods related to risk assessment, intrusion detection, SIEM/SOAR, secure architecture, digital twins, training and operational resilience can help operators and suppliers move from formal compliance claims to practical, auditable assurance. In that sense, the market opportunity lies in supporting organizations not only in implementing cybersecurity standards, but also in continuously demonstrating that these standards are effective in real power-system environments.

6.4 Training and Information Sharing

In the fast-moving environment that power grid infrastructures have to operate in, standards and regulations have a natural lag. Also, both approaches have limits in how many problems they can solve. This makes it essential for organisations to understand the benefits and limitations of standards and regulations and to develop the capabilities required to operate resilient systems beyond compliance, while embedding these requirements effectively into their operations.

Two pillars to this end are information sharing and training. Information sharing is especially important to pool resources, learn from each other’s experience, and help smaller participants to benefit from the competence and influence of the bigger ones, though it is important to assure those groups deliver sufficient quality. Training builds competences through all levels of an organisation to understand why some measures are necessary, deploy meaningful security, and increase the ability to detect and/or handle issues while they are still small.



7 References

- CENELEC. (n.d.). CLC/TC 65X-Industrial-process measurement, control and automation. Retrieved from https://standards.cenelec.eu/ords/f?p=305:22:::FSP_ORG_ID,FSP_LANG_ID:1257871,25&cs=13BBE5D228A21B7B3279EACC2D208AB42
- Jovanovic P and Neves, S. (n.d.). Practical Cryptanalysis of the Open Smart Grid Protocol. In: Leander, G. (eds) *Fast Software Encryption. FSE 2015. Lecture Notes in Computer Science()*, vol 9054. doi:10.1007/978-3-662-48116-5_15
- Kruimer, B. (10 June 2026). TRC Secure IT-OT System Architecture. *eFORT 6th General Assembly*.
- Peters, K. K. (2015). Structural Weaknesses in the Open Smart Grid Protocol. *2015 10th International Conference on Availability, Reliability and Security*, 1-10. doi:10.1109/ARES.2015.67
- Technology, N. I. (2024). Post-Quantum Cryptography Standards: FIPS 203, FIPS 204, and FIPS 205. *NIST Computer Security Resource Center*. Retrieved from https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post_Quantum_Cryptography-Standardization



ANNEX I eFORT Task 6.5 & 6.6 Questionnaire

Personal information

- What is your full name?
- For which eFORT partner company do you work?
- What eFORT task are you working on?

Task general information

- Can you explain to us what is the outcome of this task, in terms of products or KER?
- What are the main functions of your solution?
- What type of technologies do you use in your solutions?
- What benefits will it bring that are not currently brought by other tools or products in the grid?
- Will the solution improve cybersecurity or resilience of the grid?
 - ☐ Cybersecurity
 - ☐ Resilience

Regulatory compliance – Use & Implementation

- Are there any regulatory requirements that need to be considered in the use of your solution?
- Are you aware of any regulatory requirements that need to be considered for the implementation of your solution?
- Have you defined security requirements when developing the solution?
 - ☐ Yes
 - ☐ No
- Does this tool follow any of the network code or system operations guideline? (if your task is focused on resilience)

Regulatory compliance – Data

- Does your solution process data?
 - ☐ Yes
 - ☐ No
- What type of data is the solution processing? (if data is being processed)
- How does it protect sensitive grid and customer data from breaches or unauthorized access? (if sensitive data is being processed)



- How do you ensure compliance with GDPR (see <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>)? (if sensitive data is being processed)

Regulatory compliance – AI

- Does your solution use AI?
 - ☐ Yes
 - ☐ No
- What type of AI models are used in your solution? (if the solution uses AI)
- Does the AI model comply with AI regulatory frameworks such as the EU AI Act (see <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>)? (if the solution uses AI)

Standards compliance

- What standards are applicable in your country / at your demo?
- Which standards do you use?
- How do you show compliance with the standards?
- Which components are in your system that would require certification and to what standard do you foresee for that?
- What protocol communications do you use in your demo and which cyber security measures / solutions do you use?
- Do you see any gaps in standards (like IEC 62351 / 62443 or otherwise)?
- Do you see any gaps in how you can show compliance towards standards?

Conclusions

- Do you see any regulations that might hinder or improve the adoption of your solution? If so, what regulations?
- Do you see any gaps in the regulation that would help the adoption of your solution? If so, what gaps do you see?



ANNEX II Definition of Key Exploitable Results (KERs)

Table 7-1. Definition of Key Exploitable Results (KERs).

KER	KER Name	Description
1	eFORT Intelligent Platform	Tools for threat prevention, detection, and monitoring; grid adaptation algorithms; interactive visualization tool; and data sharing for collaborative response.
2	Data Base Tool	The vulnerabilities visualization tool will offer the capability for the toolbox manager, system operator or administrator to monitor EPES security state in terms of both static (user-defined, regarding current infrastructure deployed, security patches updates, etc.) and dynamic information (stemming from the prevention, detection and cyber attacks' suppression components, including the IDS, SIEM and Risk Assessment toolkits).
3	Secure Box	Embedded device for real-time cyber protection in local areas (e.g. microgrid or substation) against unauthorized access, physical manipulation, network outages, and communication disruptions.
4	Training through CRoF and digital twin of the power grids	eFORT will develop a real-time digital twin of a power grid for simulation of attacks at the cyber system layer and impact analysis at the physical layer. It will also create a training environment for red/blue team exercises and security awareness training for engineers.
6	Dynamic Risk Assessment Tools	The dynamic tool for infrastructure health analysis includes data from the EPES manager, local climate history, orographic/geographic landscape, and local business/civil ecosystem. It consists of two tools: the physical layer tool with a geo-reference feature and the cyber layer tool. -Geo-referred risk assessment tool. -Dynamic risk assessment methodology
8	IDS (Intrusion Detection System)	The IDS software detects suspicious actions compromising system security in both network and equipment using Host-Based and Network-Based Intrusion Detection Systems. Developed deep learning algorithms are configurable and updatable.
9	SIEM (Security Information and	Cloud-based software includes the server that runs the software and also storage space for log data.



KER	KER Name	Description
	Event Management)	
10	Chatbot	Interacts with energy provider users to obtain valuable information and improves grid operators' evaluation process during monitoring activities by providing aggregate information about the grid status.
11	Guide of recommendations for the safe design of substations	New security guidelines will be introduced in the substation design to prevent cyber-attacks and detect malfunctions. For existing substations, a Testbook will provide tests and checklists for cybersecurity and robustness.
12	RTU (Remote Terminal Unit)	Improvement of functionalities available in RTU as substation devices.
13	Blockchain for grid resiliency	eFORT will use blockchain to improve the resilience of the energy industry in two ways: tracing the supply chain of energy facility components and monitoring energy consumption at the TSO level to prevent attacks or failures in European networks.
14	SOAR (Security Orchestration, Automation and Response)	Open-source Security Orchestration Automation & Response (SOAR) tool for workflow driven automation of tasks in Security Operations Center (SOC). Will support a.o. CACAO and OpenC2.
15	Blueprint for EPES SOC infrastructure	For the KER 4 (Training through CRoF and digital twin of the power grids) a SOC infrastructure will be developed. This SOC infrastructure can be used as a template for EPES SOC development.
21	Connected devices vulnerabilities	Potential vulnerabilities discovered in the devices under study (e.g. HVAC, EV charging post, etc).



ANNEX III Results survey on EU regulations

As part of the analysis conducted in Task 6.6, a survey was distributed to the relevant task leaders to identify which KERs are subject to cybersecurity regulations and to gather information on how these regulatory requirements are addressed.

The survey is structured according to the different KERs. For each KER, respondents were asked to answer a set of questions using the same five-point scale: Strongly agree, Agree, Neutral, Disagree, or Strongly disagree. After each question, respondents were also asked to briefly explain the reasoning behind their chosen answer. To avoid repetition, these response options and the request for explanation are not repeated for every individual question. The following paragraphs present the structure of the survey and the results. Each topic is indicated in bold letters.

Personal information

1. What is your full name?
2. For which eFORT partner company do you work?
3. What eFORT task are you working on?
4. Which KER is relevant to you? If multiple KERs are relevant to you, please fill the questionnaire again for each KER.

KER 1: eFORT Intelligent platform

- *Question: Do you agree that the platform's threat prevention, detection, and monitoring capabilities could help prevent or minimise the impact of incidents on recipients of services, as laid out in Article 21(1) of NIS2?*

NOTE: Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

Answer: Agree. The eFORT Intelligent Platform can help support NIS2 Article 21(1) by providing monitoring, anomaly detection, alerting and event visualisation capabilities. These functions help operators detect incidents earlier and reduce their potential impact. However, the platform should be considered one technical measure within a broader set of organisational, operational and security controls required for full NIS2 compliance.

- *Question: Do you agree that the platform's detection and monitoring functions could support policies on risk analysis and information system security as well as incident handling measures, as laid out in Article 21(2)(a) and (b) of NIS2?*



NOTE: The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

- (a) policies on risk analysis and information system security;*
- (b) incident handling*

Answer: Agree. The eFORT Intelligent Platform can support NIS2 Article 21(2)(a) and (b) by providing monitoring, anomaly detection, alerting and event visualisation capabilities. These functions help provide evidence for risk analysis and support incident handling by giving operators timely and structured information. However, it should be considered a technical supporting tool within broader risk management and incident response policies, not a complete compliance solution on its own.

- *Question: Do you agree that the platform can help produce the incident reporting content (severity/impact and, where available, indicators of compromise) required by Article 23(4)(b) of NIS2?*

NOTE: Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:

(b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;

Answer: Agree. The eFORT Intelligent Platform can support the preparation of incident reporting content by collecting and visualising alerts, event data, timestamps and potential indicators of compromise. This information can help operators assess severity and impact and prepare structured incident notifications. However, the platform should be considered a supporting source of evidence, while the final NIS2 incident report and regulatory notification remain the responsibility of the relevant entity.

- *Question: Do you agree that the data sharing for collaborative response feature of the platform could support voluntary cybersecurity information sharing arrangements, as laid out in Article 29(1)(a), (b) of NIS2?*

NOTE: Member States shall ensure that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing:

- (a) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;*
- (b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.*

Answer: Agree. The eFORT Intelligent Platform can support voluntary cybersecurity information sharing by enabling partners to collect, visualise and exchange relevant



alerts, event data and indicators related to threats or anomalous behaviour. This can help improve awareness and support collaborative prevention, response and recovery activities. However, information sharing should still be governed by agreed procedures, access rules and confidentiality arrangements between the participating entities.

- *Question: Do you agree that the platform's prevention/detection/monitoring tools could support processes to identify, classify and respond to cyber-attacks that may affect cross-border electricity flows, as laid out in Article 39(1) of the NCCS?*

NOTE: Critical-impact and high-impact entities shall develop the necessary capabilities to handle detected cyber-attacks with the necessary support from the relevant competent authority, the ENTSO for Electricity and the EU DSO entity. The critical-impact and high-impact entities may be supported by the CSIRT designated in their respective Member State as part of the task assigned to the CSIRTs by Article 11(5), point (a) of Directive (EU) 2022/2555. Critical-impact and high-impact entities shall implement effective processes to identify, classify and respond to cyber-attacks that will or may affect cross-border electricity flows in order to minimise their impact.

Answer: Agree. The eFORT Intelligent Platform can support the identification, classification and response to cyber-attacks by collecting relevant security events, detecting anomalies and presenting alerts to operators. These capabilities can contribute to processes aimed at reducing the impact of incidents affecting electricity systems, including cross-border flows. However, the platform should be seen as a supporting tool within a wider operational and regulatory response framework.

- *Question: Do you agree that the interactive visualization tool of the platform could support cyber- attack management procedures with tasks and reactions based on the observable evolution of the attack, as laid out in Article 39(3)(c) of the NCCS?*

NOTE: Critical-impact and high-impact entities shall:

(c) establish cyber-attack management procedures for cyber-attacks, including roles and responsibilities, tasks and reactions based on the observable evolution of the cyber-attack within the critical-impact and high-impact perimeters;

Answer: Agree. The eFORT Intelligent Platform can support cyber-attack management procedures by providing interactive visualisation of alerts, events and their evolution over time. This helps operators understand the situation, follow the progression of an incident and support decisions on appropriate reaction tasks. However, the platform should be used as a supporting tool within predefined cyber-attack management procedures and roles.

- *Question: Do you agree that the data sharing feature of the platform could support the CSOC obligation to participate in information collection and sharing, as laid out in Article 38(1)(a) (iv) of the NCCS?*

NOTE: Each high-impact and critical-impact entity shall:

(a) establish, for all assets within its cybersecurity perimeter determined pursuant to Article 26(4) point (c), at least the CSOC capabilities to:

(iv) participate in the information collection and sharing described in this Article;



Answer: Agree. The eFORT Intelligent Platform can support CSOC information collection and sharing by collecting security events, alerts and relevant operational data, and making them available through visualisation and structured interfaces. This can help CSOC functions exchange information with relevant stakeholders. However, the platform should be considered a supporting technical tool, while formal information-sharing procedures remain the responsibility of the relevant entities.

- *Question: Do you agree that the platform could provide information on reportable cyber threats with a possible cross-border effect, as laid out in Article 38(6) of the NCCS?*

NOTE: Each critical-impact and high-impact entity shall provide without undue delay to its CSIRTs any information related to a reportable cyber threat that may have a cross-border effect. Information related to a cyber threat shall be considered reportable when at least one of the following conditions is met:

- (a) it provides relevant information for other critical-impact and high-impact entity for preventing, detecting, responding or mitigating the impact of the risk;*
- (b) the identified techniques, tactics and procedures used in the context of an attack lead to information such as compromised URL or IP addresses, hashes or any other attribute useful to contextualise and correlate the attack;*
- (c) a cyber threat may be further assessed and contextualised with additional information provided by service providers or third parties not subject to this Regulation.*

Answer: Agree. The eFORT Intelligent Platform can support the provision of information on reportable cyber threats by collecting alerts, event data and potential indicators useful for assessing and contextualising a threat. This may help relevant entities share information with CSIRTs or competent authorities when a cyber threat could have wider or cross-border impact. However, the platform should be considered a supporting source of technical evidence, while the formal assessment and reporting responsibility remains with the relevant entity.

- *Question: Do you agree that the platform's prevention/detection/monitoring capabilities could support the critical-entity risk assessment covering relevant risks including cross-sectoral, cross-border, hybrid and antagonistic threats, as laid out in Article 12(1) and 12(2) of CER?*

NOTE: 1. Notwithstanding the deadline set out in Article 6(3), second subparagraph, Member States shall ensure that critical entities carry out a risk assessment within nine months of receiving the notification referred to in Article 6(3), whenever necessary subsequently, and at least every four years, on the basis of Member State risk assessments and other relevant sources of information, in order to assess all relevant risks that could disrupt the provision of their essential services ('critical entity risk assessment').

2. Critical entity risk assessments shall account for all the relevant natural and man-made risks which could lead to an incident, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats and other antagonistic threats, including terrorist offences as provided for in Directive (EU) 2017/541. A critical entity risk assessment shall take into account the extent to which other sectors as set out in the Annex depend on the essential service provided by the critical entity and the extent to which that critical entity depends on essential services provided by other entities in such other sectors, including, where relevant, in neighbouring Member States and third countries.



Answer: Agree. The eFORT Intelligent Platform can support critical-entity risk assessment by collecting and visualising security events, anomalies and operational indicators that may be relevant to cyber, hybrid or cascading risks. This information can help entities better understand threats and dependencies affecting essential services. However, the platform should be considered a supporting technical tool, while the formal CER risk assessment remains the responsibility of the relevant critical entity.

- *Question: Do you agree that those same capabilities count as appropriate and proportionate measures to ensure resilience and prevent incidents, as laid out in Article 13(1) and 13(1)(a) of CER?*

NOTE: Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

- (a) *prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;*

Answer: Agree. The eFORT Intelligent Platform can support appropriate and proportionate resilience measures by enabling monitoring, anomaly detection, alerting and visualisation of relevant operational and cybersecurity events. These capabilities can help prevent incidents or reduce their likelihood by improving early awareness and supporting timely reaction. However, the platform should be considered one technical measure within a broader resilience framework, together with organisational, operational and security controls.

- *Question: Do you agree that the data sharing for collaborative response function of the platform could support cooperation, exchange of information and good practices, and voluntary information sharing, as laid out in Article 10(2) and 10(3) of CER?*

NOTE: 2. Each Member State shall ensure that its competent authority cooperates and exchanges information and good practices with critical entities of the sectors set out in the Annex.

3. Member States shall facilitate voluntary information sharing between critical entities in relation to matters covered by this Directive, in accordance with Union and national law on, in particular, classified and sensitive information, competition and protection of personal data.

Answer: Agree. The eFORT Intelligent Platform can support cooperation and voluntary information sharing by enabling partners to share relevant alerts, event data and cybersecurity-related information in a structured way. This can help exchange good practices and support collaborative response activities between critical entities. However, such sharing should be governed by agreed access rules, confidentiality arrangements and applicable data protection requirements.

- *Question: Do you agree that the platform, acting as a central communication hub, could support information sharing via single points of contact where incidents affect other Member States, as laid out in Article 15(3) of CER?*

NOTE: 3. On the basis of the information provided by a critical entity in a notification as referred to in paragraph 1, the relevant competent authority, via the single point of contact, shall inform the single point of contact of other affected Member States where the incident has or might have a significant impact on critical entities and the continuity of the provision of essential services to



or in one or more other Member States. Single points of contact sending and receiving information pursuant to the first subparagraph shall, in accordance with Union or national law, treat that information in a way that respects its confidentiality and protects the security and commercial interest of the critical entity concerned.

Answer: Agree. The eFORT Intelligent Platform could support information sharing by acting as a structured communication hub for alerts, event data and relevant incident information. This may help competent entities and single points of contact exchange timely information when incidents could affect other Member States. However, the platform should be considered a supporting technical tool, while formal cross-border notification and communication remain the responsibility of the relevant authorities and entities.

KER 2: Data Base Tool

- **Question:** *Do you agree that the tool's feature focusing on monitoring "static + dynamic" EPES security state could help users prioritise mitigation and so prevent or minimise incident impact, as laid out in Article 21(1) of NIS2?*

NOTE: *Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.*

Answer: Agree. Yes. The Vulnerabilities Database tool's capability to monitor the EPES security state using both static and dynamic vulnerability data can help users prioritise mitigation actions and, therefore, prevent or minimise the impact of incidents, in line with the risk-management logic of Article 21(1) of NIS2. The tool supports this by combining static vulnerability intelligence, such as known vulnerabilities, severity information and affected products or services, with dynamic EPES-specific information, such as asset characteristics, exposure, criticality and evolving vulnerability status. This allows users to move beyond a generic list of vulnerabilities and understand which weaknesses are most relevant for the specific EPES infrastructure under consideration. In practice, this can help operators and cybersecurity teams identify vulnerable assets, assess which vulnerabilities may have the highest operational impact, and prioritise mitigation measures accordingly. For example, vulnerabilities affecting critical nodes, exposed services, OT-to-IT interfaces or assets with higher potential impact on power-system operation can be treated with higher priority than less critical findings. This supports proportionate decision-making, where mitigation actions are selected based on risk exposure, likelihood and potential severity. Therefore, the tool contributes to the technical and operational measures expected under Article 21(1), especially regarding risk management and the prevention or minimisation of incident impact. However, it should be noted that the tool is an enabling component: full alignment with NIS2 also



requires organisational procedures, responsibilities, remediation workflows, governance and periodic review mechanisms to ensure that the identified mitigation priorities are actually acted upon.

- *Question: Do you agree that the tool's visibility on vulnerabilities and patches could support security in acquisition/development/maintenance including vulnerability handling, as laid out in Article 21(2)(e) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

Answer: Agree. The Vulnerabilities Database tool's visibility on vulnerabilities and patches can support security in network and information systems acquisition, development and maintenance, including vulnerability handling, as required under Article 21(2)(e) of NIS2. The tool provides a structured view of known vulnerabilities affecting relevant EPES assets, components, software, firmware and services. By linking vulnerability information with affected products, severity, exploitability, references, mitigation guidance and potential patch availability, it can help users understand whether a component or system has known weaknesses and what actions may be required to address them. This is relevant during acquisition, because users can take vulnerability exposure and vendor patch availability into account when selecting or accepting new equipment, software or services. It is also relevant during development, because known vulnerabilities and weakness categories can inform secure design, configuration, testing and integration decisions. During maintenance, the tool can support vulnerability handling by helping operators identify affected assets, prioritise remediation, plan patching or compensating controls, and keep evidence of the vulnerability management process. Therefore, the tool contributes to the technical and operational measures expected by Article 21(2)(e), particularly in relation to vulnerability handling and patch management. However, full compliance would also require organisational procedures for vulnerability disclosure, supplier coordination, patch validation, change management, approval workflows and documentation of remediation actions.

- *Question: Do you agree that the single combined view of the platform could support the entity-level risk assessment requirement to consider assets, vulnerabilities (including legacy), threats, scenarios and controls, as laid out in Article 26(4)(a)(i) to (vi) of the NCCS?*

NOTE: 4. During the cybersecurity risk assessment phase, each high-impact and critical-impact entity shall:

(a) identify cybersecurity risks by taking into account:

- (i) all assets supporting the Union-wide high-impact and critical-impact processes with an assessment of the possible impact on cross-border electricity flows if the asset is compromised;*
- (ii) possible cyber threats taking into account the cyber threats identified in the latest Comprehensive cross-border electricity cybersecurity risk assessment report referred to in Article 23 and supply chain threats;*
- (iii) vulnerabilities, including vulnerabilities in legacy systems;*



(iv) possible cyber-attack scenarios, including cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows;

Answer: Agree. Yes. The single combined view of the platform can support the entity-level cybersecurity risk assessment requirement described in Article 26(4)(a)(i)–(vi) of the NCCS. The combined platform view brings together several elements that are needed for a structured risk assessment: assets, vulnerabilities, threats, attack scenarios, security events, and possible mitigation or control options. This is particularly relevant for EPES environments, where cybersecurity risk cannot be assessed only at the level of individual IT systems, but must also consider OT assets, power-grid nodes, communication interfaces and possible operational impacts. With respect to assets, the platform can provide visibility over EPES components, sectors and nodes, including information that may be relevant for assessing the possible impact of compromise. With respect to vulnerabilities, the Vulnerabilities Database can help identify known weaknesses affecting specific assets, including older or legacy systems where such assets are registered and vulnerability information is available. With respect to threats and cyber-attack scenarios, the platform can combine vulnerability intelligence with monitoring information, alerts, attack patterns and threat-modelling outputs. Finally, with respect to controls, the platform can help users understand which mitigation measures or defence actions may be relevant before applying them. Therefore, the single combined view can act as a practical decision-support layer for the risk assessment required by the NCCS, because it helps users correlate what assets exist, how exposed they are, which vulnerabilities and threats are relevant, what scenarios could affect operational security, and which controls may reduce the risk. However, full compliance with Article 26 would still require the entity to complement the tool output with formal risk governance, documented assumptions, cross-border electricity-flow impact analysis, risk acceptance criteria and periodic review.

- *Question: Do you agree that the tool's records of vulnerabilities, patch state, alerts and risk outputs could support CSOC security logging, monitoring, intrusion detection and vulnerability assessment, as laid out in Article 38(1)(a)(i) and (ii) of the NCCS?*

NOTE: Each high-impact and critical-impact entity shall:

(a) establish, for all assets within its cybersecurity perimeter determined pursuant to Article 26(4) point (c), at least the CSOC capabilities to:

(i) ensure that the relevant network and information systems and applications provide security logs for security monitoring to enable the detection of anomalies and collect information on cyber-attacks;

(ii) conduct security monitoring, including detecting intrusions and assessing vulnerabilities of network and information systems;

Answer: Agree. Yes. The tool's records of vulnerabilities, patch state, alerts and risk outputs can support the CSOC capabilities described in Article 38(1)(a)(i)–(ii) of the NCCS, particularly when used as part of the integrated eFORT platform together with the SIEM and IDS components. The tool supports vulnerability assessment by maintaining structured information on known vulnerabilities, affected assets, severity, mitigation guidance and patch-related status. This allows cybersecurity teams and CSOC operators to identify exposed systems, assess the relevance and criticality of



vulnerabilities, and prioritise remediation or compensating controls. In addition, when integrated with the SIEM/IDS layer, the same information can be correlated with security logs, alerts, network traffic analysis and asset health indicators. This supports security monitoring by enabling operators to detect anomalies, relate alerts to vulnerable assets, and understand whether a detected event may have higher operational risk due to unpatched or exposed weaknesses. Therefore, the combined view can contribute to the CSOC's ability to collect and use security logs, monitor network and information systems, detect intrusions and assess vulnerabilities. However, the tool should be considered an enabling capability rather than a complete CSOC by itself. Full compliance with Article 38 would also require appropriate deployment coverage across all in-scope assets, log-retention policies, operational CSOC procedures, alert triage workflows, escalation processes and qualified personnel.

- *Question: Do you agree that the tool's static information (current infrastructure deployed and security patch updates) could support preventing incidents, as laid out in Article 13(1)(a) of CER?*

NOTE: Member States shall ensure that critical entities take appropriate and proportionate technical, security and

organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

- (a) prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;*

Answer: Agree. Yes. The tool's static information on the current EPES infrastructure and security patch updates can support the prevention of incidents, as described in Article 13(1)(a) of the CER Directive. By maintaining visibility over deployed assets, known vulnerabilities, affected products or services, and patch or mitigation status, the tool helps users identify weaknesses before they are exploited. This supports preventive cybersecurity action, because operators can determine which assets are exposed, which systems require patching or compensating controls, and which vulnerabilities may create higher risk for critical EPES operations. The tool can therefore contribute to appropriate and proportionate technical and organisational measures aimed at resilience. In practice, it can support asset inventory maintenance, vulnerability tracking, patch prioritisation, system hardening and planning of preventive maintenance actions. For EPES environments, where immediate patching may not always be possible due to operational constraints, the tool can also help identify temporary mitigations, such as disabling vulnerable services, filtering communications, increasing monitoring or planning controlled patching windows. Therefore, we agree that the tool can support the prevention of incidents under Article 13(1)(a). However, it should be considered an enabling cybersecurity component rather than a complete CER resilience solution. Full alignment with Article 13 would also require wider organisational resilience measures, physical security, continuity planning, disaster risk reduction and climate adaptation measures.

- *Question: Do you agree that the dynamic information from prevention/detection/suppression components could support responding to,*



resisting and mitigating the consequences of incidents, as laid out in Article 13(1)(c) of CER?

NOTE: Member States shall ensure that critical entities take appropriate and proportionate technical, security and

organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

- (b) respond to, resist and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;*

Answer: Agree. Yes. The dynamic information received from prevention, detection and suppression components can support the ability of critical entities to respond to, resist and mitigate the consequences of incidents, as described in Article 13(1)(c) of the CER Directive. The Vulnerabilities Database tool does not only provide static knowledge of known vulnerabilities; when integrated with dynamic inputs from monitoring, detection and mitigation components, it can help users understand how vulnerabilities relate to live alerts, affected assets, attack patterns, node status and operational risk. This enables cybersecurity teams to move from generic vulnerability awareness to incident-oriented decision support. In practice, such dynamic information can support response and mitigation by helping users identify which assets are affected, which vulnerabilities may be exploited, what the likely severity or impact is, and which mitigation actions or compensating controls should be prioritised. When correlated with SIEM alerts, IDS findings and mitigation feedback, the tool can support faster triage, better situational awareness and more targeted response actions. Therefore, we agree that the tool can contribute to the measures described in Article 13(1)(c), especially regarding alert routines, incident response support, risk-based mitigation and reduction of incident consequences. However, it should be considered an enabling technical component rather than a complete crisis-management framework. Full alignment with Article 13(1)(c) would also require documented incident response procedures, escalation protocols, roles and responsibilities, crisis-management plans, communication routines and regular exercises.

- *Question: Do you agree that the tool's records of vulnerabilities, patch state, alerts and risk outputs can serve as evidence that resilience measures meet Article 13 and are effectively implemented, as laid out in Article 21(2)(a) and (b) of CER?*

NOTE: Article 21(2)(a),(b):

Member States shall ensure that the competent authorities have the powers and means to require, where necessary for the performance of their tasks under this Directive, that the entities under Directive (EU) 2022/2555 that Member States have identified as critical entities under this Directive provide, within a reasonable time limit set by those authorities:

- (a) the information necessary to assess whether the measures taken by those entities to ensure their resilience meet the requirements set out in Article 13;*
- (b) evidence of the effective implementation of those measures, including the results of an audit conducted by an independent and qualified auditor selected by that entity and conducted at its expense.*



Answer: Agree. Yes. The tool's records of vulnerabilities, patch state, alerts and risk outputs can support the provision of information and evidence requested under Article 21(2)(a) and (b) of the CER Directive. The tool can provide documented evidence of the cybersecurity and resilience measures applied to the EPES infrastructure, including which assets were monitored, which vulnerabilities were identified, how critical they were, whether patches or updates were required, which alerts were generated, and how risks evolved over time. This information can help demonstrate that the entity is not only aware of its risk exposure, but also maintains a structured process for vulnerability management, monitoring, prioritisation and mitigation. Such records can therefore support competent authorities or auditors in assessing whether the measures taken by the entity meet the resilience requirements of Article 13. For example, vulnerability records, patch-status information, risk outputs and alert histories can show whether preventive, monitoring and mitigation measures are being applied in practice and whether they are proportionate to the risks identified. However, the tool should be considered as an evidence-generating and audit-supporting mechanism, not as a complete compliance mechanism by itself. Full alignment with Article 21(2)(a) and (b) would also require documented organisational procedures, management approvals, remediation records, independent audit results, and evidence that identified measures were actually implemented and maintained over time.

KER 3: Secure Box

- *Question: Do you agree that the box's unauthorised access protection could support access control policies and asset management, as laid out in Article 21(2)(i) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

- (i) *human resources security, access control policies and asset management;*

Answer: Agree. SecureBox can help enforce access restrictions and protect substation assets from unauthorised use, supporting access control and asset protection. It should still be complemented by formal policies, user management, and asset inventories.

- *Question: Do you agree that by reducing the likelihood of local compromise escalating into wider disruption, the Secure Box could help minimise incident impact, as laid out in Article 21(1) of NIS2?*

NOTE: Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.



Answer: Agree. SecureBox can help contain local compromise and reduce the risk of wider disruption to substation operations and connected services. Its impact depends on correct deployment, integration, and response procedures.

- *Question: Do you agree that the box's protection against physical manipulation could support the all-hazards protection of systems and their physical environment, as laid out in Article 21(2) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents (...).

Answer: Agree. SecureBox can help protect substation systems against physical tampering and manipulation, supporting the all-hazards approach. It should complement wider physical security, monitoring, and incident-response measures.

- *Question: Do you agree that the box's resilience to network outages and communication disruptions could support business continuity, as laid out in Article 21(2)(c) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

- (c) *business continuity, such as backup management and disaster recovery, and crisis management;*

Answer: Agree. SecureBox can help maintain substation protection and monitoring during communication disruptions, supporting continuity and crisis management. It should still be complemented by backup, recovery, and operational continuity procedures.

- *Question: Do you agree that local hardening at substation/microgrid level of the box could support defining high/critical-impact perimeters so access can be controlled, as laid out in Article 26(4)(c)(iv) of the NCCS?*

NOTE: 4. During the cybersecurity risk assessment phase, each high-impact and critical-impact entity shall:

(c) classify assets according to the possible consequences when cybersecurity is compromised and determine the high-impact and critical-impact perimeter using the following steps:

(iv) define the high-impact and critical-impact perimeters containing all high-impact and critical-impact assets respectively, so that access to the perimeters may be controlled;

Answer: Agree. SecureBox can help enforce and evidence local security boundaries at substation or microgrid level, supporting perimeter definition and access control. It should complement formal perimeter mapping, asset classification, and governance.

- *Question: If physical tampering is treated as a pathway that enables cyber compromise of substation ICT assets, do you agree that the physical-manipulation protection feature of the SecureBox could reduce vulnerabilities and strengthen the protection of assets considered in the entity-level risk assessment, as laid out in Article 26(4)(a)(iii) of the NCCS?*



NOTE: 4. During the cybersecurity risk assessment phase, each high-impact and critical-impact entity shall:

(a) identify cybersecurity risks by taking into account:

(iii) vulnerabilities, including vulnerabilities in legacy systems;

Answer: Agree. SecureBox can reduce tampering-related vulnerabilities that could enable cyber compromise of substation ICT assets. It should be considered alongside legacy-system risks, technical controls, and the wider entity-level risk assessment.

- **Question:** Do you agree that physical-manipulation prevention could be an incident-prevention measure, as laid out in Article 13(1)(a) of CER?

NOTE: Member States shall ensure that critical entities take appropriate and proportionate technical, security and

organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

- (a) prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;

Answer: Agree. Preventing physical manipulation can reduce the likelihood of incidents affecting substation assets and service continuity.

- **Question:** Do you agree that the protection against physical manipulation feature of the SecureBox could support adequate physical protection of premises and critical infrastructure, as laid out in Article 13(1)(b) of CER?

NOTE: Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

(b) ensure adequate physical protection of their premises and critical infrastructure, duly considering, for

example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls;

Answer: Disagree. SecureBox's physical-manipulation protection mainly protects the device itself, rather than the wider premises or other critical infrastructure assets. It may provide limited support, but adequate physical protection still requires broader measures such as perimeter monitoring, access controls, barriers, and site security procedures.

KER 4: Training through CRoF and digital twin of the power grids

- **Question:** Do you agree that the training environment could help meet the basic cyber hygiene practices and cybersecurity training, as laid out in Article 21(2)(g) of NIS2?

NOTE: The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(g) basic cyber hygiene practices and cybersecurity training;



Answer: Strongly agree. The CRoF environment provides hands-on cybersecurity awareness, incident-response practice, and operator training in realistic cyber-physical scenarios, so it directly supports cyber hygiene and cybersecurity training.

- *Question: Do you agree that building practical skills to handle realistic scenarios could help prevent or minimise incident impact, as laid out in Article 21(1) of NIS2?*

NOTE: Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

Answer: Strongly agree. Realistic CRoF scenarios help operators and security staff practise detection, coordination, mitigation, and recovery, which can help prevent incidents and reduce their operational impact.

- *Question: Do you agree that, if used for management bodies, the training could support the requirement for members of management bodies to follow training, as laid out in Article 20(2) of NIS2?*

NOTE: Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Answer: Agree. The platform can support management training by improving understanding of cyber risks, operational dependencies, and cybersecurity risk-management decisions, although it is primarily designed for operators and technical staff.

- *Question: Do you agree that the exercise environment could support the cybersecurity exercise that critical-impact entities must perform every three years, as laid out in Article 43(1) of the NCCS?*

NOTE: By 31 December of the year after the notification of critical-impact entities, and every three years thereafter, each critical-impact entity shall perform a cybersecurity exercise including one or more scenarios with cyber-attacks affecting cross-border electricity flows directly or indirectly and related to the risks identified during the cybersecurity risk assessments at Member State and entity levels in accordance with Article 20 and Article 27.

Answer: Agree. The environment supports realistic TSO/OT cyber-physical exercise scenarios, operator workflows, and evaluation, so it can support the required periodic NCCS exercises, although full compliance also depends on organisational setup and exercise governance.



- *Question: Do you agree that it could support participation in the regional/cross-regional exercises held every three years, as laid out in Article 44(1) of the NCCS?*

NOTE: By 31 December 2029, and every three years thereafter, in each system operation region, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall organise a regional cybersecurity exercise. The critical-impact entities in the system operation region shall participate in the regional cybersecurity exercise. The ENTSO for Electricity, in cooperation with the EU DSO entity, may organise, instead of a regional cybersecurity exercise, a cross regional cybersecurity exercise in more than one system operating regions in the same timeframe. The exercise should take into account other existing cybersecurity risk assessments and scenarios developed at Union level.

Answer: Agree. The platform can support regional or cross-regional exercises because it provides representative grid, OT, and incident-response scenarios, but broader multi-entity coordination would still need to be organised around it.

- *Question: Do you agree that the digital twin/exercise environment could help generate the evidence and lessons learned for the exercise outcomes report, as laid out in Article 45(2) of the NCCS?*

NOTE: The organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1), with the advice of ENISA if requested by them and pursuant to Article 7(5) of Regulation (EU) 2019/881, shall analyse and finalise the relevant cybersecurity exercise through a report summarising the lessons, addressed to all participants. The report shall include:

(a) the exercise scenarios, meeting reports, main positions, successes and lessons learnt at any level of the electricity value chain;

(b) whether the key success criteria were met;

(c) a list of recommendations for entities participating in the relevant cybersecurity exercise to correct, adapt or change cybersecurity crisis processes, procedures, associated governance models and any existing contractual engagements with critical service providers.

Answer: Strongly agree. The CRoF and digital twin environment can generate scenarios, operator action logs, KPIs, debrief inputs, survey feedback, and lessons learned, which are exactly the kind of evidence needed for exercise outcome reports.

- *Question: Do you agree that the training could support building the cybersecurity skills staff need to comply with the CRA, as described in Recital 23 of the CRA?*

NOTE: The effectiveness of the implementation of this Regulation will also depend on the availability of adequate cybersecurity skills. At Union level, various programmatic and political documents, including the Commission communication of 18 April 2023 on Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience and the Council Conclusions of 22 May 2023 on the EU Policy on Cyber Defence acknowledged the cybersecurity skills gap in the Union and the need to address such challenges as a matter of priority, in both the public and private sectors. With a view to ensuring an effective implementation of this Regulation, Member States should ensure that adequate resources are available for the appropriate staffing of the market surveillance authorities and conformity assessment bodies to perform their tasks as laid down in this Regulation. Those measures should enhance workforce mobility in the cybersecurity field and their associated career pathways. They should also contribute to making the cybersecurity workforce more resilient and inclusive, also in terms of



gender. Member States should therefore take measures to ensure that those tasks are carried out by adequately trained professionals, with the necessary cybersecurity skills. Similarly, manufacturers should ensure that their staff has the necessary skills to comply with their obligations as laid down in this Regulation. Member States and the Commission, in line with their prerogatives and competences and the specific tasks conferred upon them by this Regulation, should take measures to support manufacturers and in particular microenterprises and small and medium-sized enterprises, including start-ups, also in areas such as skill development, for the purposes of compliance with their obligations as laid down in this Regulation. Furthermore, as Directive (EU) 2022/2555 requires Member States to adopt policies promoting and developing training on cybersecurity and cybersecurity skills as part of their national cybersecurity strategies, Member States may also consider, when adopting such strategies, addressing the cybersecurity skills needs resulting from this Regulation, including those relating to re-skilling and up-skilling.

Answer: Agree. The training helps staff build relevant cybersecurity skills in monitoring, incident handling, and coordinated response, although CRA-specific product compliance would still require additional product-focused training.

- **Question:** Do you agree that the training and exercises could support raising awareness among relevant personnel, as laid out in Article 13(1)(f) of CER?

NOTE: Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

(f) raise awareness about the measures referred to in points (a) to (e) among relevant personnel, duly considering training courses, information materials and exercises.

Answer: Strongly agree. The training and exercises raise awareness among relevant personnel by exposing them to realistic attack paths, operational impacts, mitigation choices, and recovery actions in a structured environment.

- **Question:** Do you agree that the training could support employee security management including training requirements and qualifications, as laid out in Article 13(1)(e) of CER?

NOTE: Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

- (d) ensure adequate employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, setting up procedures for background checks in accordance with Article 14 and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications;

Answer: Agree. The platform supports the training and qualification part of employee security management well, but it does not by itself cover broader CER measures such as access-rights governance or background-check procedures.

- **Question:** Do you agree that the exercise environment could support the organisation of exercises to test resilience, as laid out in Article 10(1) of CER?



NOTE: Member States shall support critical entities in enhancing their resilience. That support may include developing guidance materials and methodologies, supporting the organisation of exercises to test their resilience and providing advice and training to the personnel of critical entities. Without prejudice to applicable rules on State aid, Member States may provide financial resources to critical entities, where necessary and justified by public interest objectives.

Answer: Agree. The exercise environment is specifically suited to resilience testing because it combines cyber range activities, operator decision support, digital-twin analysis, and restoration workflows in realistic power-grid scenarios.

KER 6: Dynamic Risk Assessment Tools

- *Question: Do you agree that the geo-referred multi-layer (physical and cyber) risk assessment could support an all-hazards approach and policies on risk analysis and information system security, as laid out in Article 21(2) and 21(2)(a) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all- hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

Answer 1: Neutral. As both the RINA and EMI components of the Dynamic Risk Assessment Tools focus on the physical layer, they are designed to evaluate physical hazards. Furthermore, the Dynamic Security Assessment tool (EMI) assesses the consequences of general outages, meaning it can also support the analysis of events triggered by cyberattacks.

Answer 2: Strongly agree. The geo-referred hazard quantification is very important for the risk assessment.

- *Question: Do you agree that the geo-referred asset/location view could support identifying assets, classifying them and defining perimeters for access control, as laid out in Article 26(4)(a)(i) and (c)(iii) to (iv) of the NCCS?*

NOTE: 4. During the cybersecurity risk assessment phase, each high-impact and critical-impact entity shall:

(a) identify cybersecurity risks by taking into account:

(i) all assets supporting the Union-wide high-impact and critical-impact processes with an assessment of the possible impact on cross-border electricity flows if the asset is compromised
Article 26(c)(iii)-(iv):(c) classify assets according to the possible consequences when cybersecurity is compromised and determine the high-impact and critical-impact perimeter using the following steps:

(iii) determine all high-impact and critical-impact assets as the assets needed for the high-impact and critical-impact processes respectively;

(iv) define the high-impact and critical-impact perimeters containing all high-impact and critical-impact assets respectively, so that access to the perimeters may be controlled;

Answer 1: Neutral. Since this question rather addresses a tool developed by RINA, I would prefer to leave it to them.



Answer 2: Strongly agree. Can be useful for ranking the level of risk and define potential mitigation measure based on the prioritized assets.

- *Question: Do you agree that the dynamic methodology could support analysing likelihood and consequences and determining the risk level using the risk impact matrix, as laid out in Article 26(4)(b) of the NCCS?*

NOTE: During the cybersecurity risk assessment phase, each high-impact and critical-impact entity shall:

- (b) *analyse the likelihood and consequences of the cybersecurity risks identified in point (a) and determine the cybersecurity risk level using the risk impact matrix used to assess cybersecurity risks in cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level developed by TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity in accordance with Article 19(2);*

Answer 1: Strongly agree. The Dynamic Security Assessment tool can assess the consequences of disruption events resulting from cyberattacks.

Answer 2: Agree. Is important in risk analysis to consider hazard, vulnerability (how the asset behave against different hazard intensities) and potential exposure (physical damage quantification and service interruption economic losses).

- *Question: Do you agree that the tool could support the recurring (at least every four years) risk assessment of all relevant disrupting risks, as laid out in Article 12(1) of CER?*

NOTE: Notwithstanding the deadline set out in Article 6(3), second subparagraph, Member States shall ensure that critical entities carry out a risk assessment within nine months of receiving the notification referred to in Article 6(3), whenever necessary subsequently, and at least every four years, on the basis of Member State risk assessments and other relevant sources of information, in order to assess all relevant risks that could disrupt the provision of their essential services ('critical entity risk assessment').

Answer 1: Disagree. The geo-referred physical risk assessment tool (RINA) might be suitable. The Dynamic Security Assessment tool (EMI) is not suitable for this task...

Answer 2: Strongly agree. True.

- *Question: Do you agree that the climate data and the RINA-C tool could support an all-hazards methodology covering natural disasters and cross-border dependencies, as laid out in Article 12(2) of CER?*

NOTE: 2. Critical entity risk assessments shall account for all the relevant natural and man-made risks which could lead to an incident, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats and other antagonistic threats, including terrorist offences as provided for in Directive (EU) 2017/541. A critical entity risk assessment shall take into account the extent to which other sectors as set out in the Annex depend on the essential service provided by the critical entity and the extent to which that critical entity depends on essential services provided by other entities in such other sectors, including, where relevant, in neighbouring Member States and third countries.

Answer 1: Neutral. Since this question specifically addresses a tool developed by RINA, I would prefer to leave it to them.



Answer 2: Agree. Climate data can give an overview of how the risk can increase for future prediction hazard models.

KER 8: IDS (Intrusion Detection System)

- *Question: Do you agree that detecting suspicious actions in networks and equipment could support incident handling, as laid out in Article 21(2)(b) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(c) incident handling;

Answer: Strongly agree. Detecting suspicious activity in networks and equipment is a direct input to incident handling because it helps identify potential incidents early, assess their scope, prioritize response, and support containment and remediation actions.

- *Question: Do you agree that faster detection and triage could help minimise incident impact, as laid out in Article 21(1) of NIS2?*

NOTE: Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

Answer: Strongly agree. Faster detection and triage help organisations understand incidents earlier, prioritize the response, contain threats sooner, and reduce operational, financial, and security impact.

- *Question: Do you agree that the IDS monitoring output could feed the incident notification content (severity/impact and indicators of compromise), as laid out in Article 23(4)(b) of NIS2?*

NOTE: Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:

- (b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;*

Answer: Strongly agree. IDS monitoring output can provide useful notification content such as affected systems, alert severity, timestamps, attack indicators, and available IOCs. It should still be validated and correlated with other evidence before being used in an official incident notification.



- *Question: Do you agree that the IDS could provide CSOC security monitoring including intrusion detection, as laid out in Article 38(1)(a)(ii) of the NCCS?*

NOTE: Each high-impact and critical-impact entity shall:

(a) establish, for all assets within its cybersecurity perimeter determined pursuant to Article 26(4) point (c), at least the CSOC capabilities to:

(ii) conduct security monitoring, including detecting intrusions and assessing vulnerabilities of network and information systems;

Answer: Strongly agree. Intrusion detection is a core IDS function, so an IDS can directly support CSOC security monitoring by identifying suspicious or malicious activity. It should be integrated with wider CSOC processes such as alert triage, investigation, vulnerability assessment, and response.

- *Question: Do you agree that the IDS could help systems provide security logs for monitoring and anomaly detection, as laid out in Article 38(1)(a)(i) of the NCCS?*

NOTE: Each high-impact and critical-impact entity shall:

(a) establish, for all assets within its cybersecurity perimeter determined pursuant to Article 26(4) point (c), at least the CSOC capabilities to:

(i) ensure that the relevant network and information systems and applications provide security logs for security monitoring to enable the detection of anomalies and collect information on cyber-attacks;

Answer: Agree. An IDS can generate alerts, telemetry, and event data that support monitoring, anomaly detection, and cyber-attack analysis. However, it complements rather than replaces logs from systems, applications, endpoints, firewalls, and identity platforms.

- *Question: Do you agree that IDS alerts could support identifying, classifying and responding to cyber- attacks affecting cross-border flows, as laid out in Article 39(1) of the NCCS?*

NOTE: Critical-impact and high-impact entities shall develop the necessary capabilities to handle detected cyber-attacks with the necessary support from the relevant competent authority, the ENTSO for Electricity and the EU DSO entity. The critical-impact and high-impact entities may be supported by the CSIRT designated in their respective Member State as part of the task assigned to the CSIRTs by Article 11(5), point (a) of Directive (EU) 2022/2555. Critical-impact and high-impact entities shall implement effective processes to identify, classify and respond to cyber-attacks that will or may affect cross-border electricity flows in order to minimise their impact.

Answer: Agree. IDS alerts can provide early evidence of suspicious activity, help classify the type and severity of an attack, and support response decisions. However, assessing impact on cross-border flows also requires operational context, coordination, and incident-response processes beyond the IDS itself.

- *Question: Do you agree that configurable/updatable detection could support performance evaluation and continual improvement, as laid out in Article 32(1)(i) to (k) of the NCCS?*

NOTE: Within 24 months after being notified by the competent authority that they have been identified as a high-impact or critical-impact entity in accordance with Article 24(6), each high-



impact and critical-impact entity shall establish a cybersecurity management system, and review it every three years thereafter, to:

- (i) create, update and control documented information related to the cybersecurity management system;*
- (j) evaluate the performance and effectiveness of the cybersecurity management system;*
- (k) conduct internal audits at planned intervals to ensure that the cybersecurity management system is effectively implemented and maintained;*

Answer: Agree. Configurable and updatable detection rules support tuning, documentation, effectiveness reviews, and audit evidence. They help improve detection performance over time, but they are only one part of the broader cybersecurity management system.

KER 9: SIEM

- **Question:** *Do you agree that the SIEM could support incident handling, as laid out in Article 21(2)(b) of NIS2?*

NOTE: *The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following: (b) incident handling;*

Answer: Agree. Yes. The SIEM can support incident handling, as required under Article 21(2)(b) of NIS2. The SIEM provides a centralised capability for collecting, aggregating, correlating and analysing security-relevant information from IT and OT assets. In the EPES context, this includes logs, alerts, IDS findings, network traffic information, vulnerability-related data and asset health indicators. By correlating these inputs, the SIEM can help detect suspicious activity, classify events, generate alerts and provide security operators with a clearer view of potential incidents. This supports incident handling because it enables faster identification, triage, investigation and prioritisation of cybersecurity events. In addition, the eSIEM is integrated with response-oriented capabilities, including alerting, node health assessment, mitigation support, the Fast Mitigation System and SOAR/playbook-based response mechanisms. These functions can help operators move from detection to coordinated response, containment and mitigation. Therefore, we agree that the SIEM supports the incident-handling measures referred to in Article 21(2)(b) of NIS2. However, the SIEM should be considered an enabling technical capability rather than the full incident-handling process by itself. Complete alignment with NIS2 would also require documented incident-response procedures, defined roles and responsibilities, escalation paths, communication routines, reporting obligations, post-incident review and regular testing of the incident-response process.

- **Question:** *Do you agree that the SIEM could support producing the incident notification content (severity/impact and indicators of compromise), as laid out in Article 23(4)(b) of NIS2?*

NOTE: *Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:*

- (b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information*



referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;

Answer: Agree. Yes. The SIEM can support the production of incident notification content required under Article 23(4)(b) of NIS2, including the initial assessment of severity and impact and, where available, indicators of compromise. The SIEM collects and correlates security-relevant information from multiple IT and OT sources, including system logs, user activity, network traffic, IDS findings, alerts, vulnerabilities, asset health indicators and MITRE ATT&CK mappings. This information can help security teams reconstruct what happened, identify the affected assets, assess whether the event is significant, and estimate the potential severity and impact of the incident. The SIEM can also support the identification of indicators of compromise by providing evidence such as suspicious events, abnormal network activity, malicious or anomalous behaviour, affected nodes, file-integrity changes, related vulnerabilities, attack patterns and mapped adversary techniques. These outputs can form the technical basis for the 72-hour incident notification required by NIS2. Therefore, we agree that the SIEM can support the preparation of incident notification content under Article 23(4)(b). However, the SIEM should be considered an enabling evidence and reporting-support tool, not a replacement for the formal notification process. The final assessment, legal qualification of the incident, approval and submission to the CSIRT or competent authority should remain under the responsibility of the entity's incident-response and compliance procedures.

- *Question: Do you agree that SIEM data and reports could serve as evidence of implementation that authorities may request, as laid out in Article 32(2)(e) to (g) and 33(2)(d) to (f) of NIS2?*

NOTE: 32(2). Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to:

(e) requests for information necessary to assess the cybersecurity risk- management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;

(f) requests to access data, documents and information necessary to carry out their supervisory tasks;

(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

33(2). Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to:

(d) requests for information necessary to assess, ex post, the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;

(e) requests to access data, documents and information necessary to carry out their supervisory tasks;



(f) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out.

Answer: Agree. Yes. SIEM data and reports can support the provision of information, data, documents and evidence of implementation that competent authorities may request under Articles 32(2)(e)–(g) and 33(2)(d)–(f) of NIS2. The SIEM collects and stores security-relevant information from the monitored IT and OT environment, including logs, event records, alerts, IDS findings, vulnerability assessments, configuration information and asset-related security indicators. These records can help demonstrate that cybersecurity risk-management measures are not only defined, but also operationally implemented and monitored in practice. For example, SIEM dashboards and reports can provide evidence that security logging is active, that alerts are generated and reviewed, that anomalies and intrusions are detected, that vulnerabilities are assessed, and that mitigation or response actions are triggered or tracked. This type of information can support supervisory requests for data and documents, as well as requests for evidence showing how cybersecurity policies and controls are applied in the actual infrastructure. Therefore, we agree that SIEM data and reports can serve as useful evidence for supervisory and audit purposes under NIS2. However, they should be considered part of the underlying evidence base rather than a complete compliance package by themselves. Full evidence of implementation would also require documented cybersecurity policies, risk-management procedures, audit results, remediation records, roles and responsibilities, approvals, and governance documentation.

- *Question: Do you agree that the cloud SIEM could provide one place to collect and retain security logs for monitoring and anomaly detection, as laid out in Article 38(1)(a)(i) of the NCCS?*

NOTE: Each high-impact and critical-impact entity shall:

(a) establish, for all assets within its cybersecurity perimeter determined pursuant to Article 26(4) point (c), at least the CSOC capabilities to:

(i) ensure that the relevant network and information systems and applications provide security logs for security monitoring to enable the detection of anomalies and collect information on cyber-attacks;

Answer: Agree. Yes. The cloud SIEM could provide a centralised place to collect, retain and analyse security logs for monitoring and anomaly detection, as required under Article 38(1)(a)(i) of the NCCS. The SIEM is designed to collect security-relevant information from distributed IT and OT assets, including system logs, service activity, file-integrity information, IDS findings and network-traffic data. In a cloud deployment, these data sources can be forwarded to a central SIEM environment where they are stored, indexed, correlated and visualised. This supports the CSOC capability to monitor relevant network and information systems and applications, detect anomalies, and collect information related to cyber-attacks. For EPES environments, this is particularly useful because assets may be distributed across substations, control-centre systems, cloud services, virtual machines, containers and other operational components. A cloud SIEM can provide a unified monitoring and log-retention layer across these heterogeneous environments, enabling security operators to investigate events, correlate alerts and maintain historical evidence. Therefore, we agree that the cloud SIEM can support Article 38(1)(a)(i). However, full alignment would require that all assets within the defined



cybersecurity perimeter are actually connected or otherwise covered, that log-retention periods and integrity protections are defined, that sensitive OT data is securely transmitted and stored, and that access control, data residency and incident-response procedures are properly governed.

- *Question: Do you agree that centralised logs could help investigate, classify and document cyber- attacks, as laid out in Article 39(1) of the NCCS?*

NOTE: Critical-impact and high-impact entities shall develop the necessary capabilities to handle detected cyber-attacks with the necessary support from the relevant competent authority, the ENTSO for Electricity and the EU DSO entity. The critical-impact and high-impact entities may be supported by the CSIRT designated in their respective Member State as part of the task assigned to the CSIRTs by Article 11(5), point (a) of Directive (EU) 2022/2555. Critical-impact and high-impact entities shall implement effective processes to identify, classify and respond to cyber-attacks that will or may affect cross-border electricity flows in order to minimise their impact.

Answer: Agree. Yes. Centralised logs can help investigate, classify and document cyber-attacks, as required under Article 39(1) of the NCCS. A SIEM provides a central point for collecting, correlating and retaining security-relevant information from distributed IT and OT assets, including system logs, network events, IDS findings, alerts, vulnerability information and asset-related indicators. This allows security teams to reconstruct the sequence of events, identify affected assets, understand how an attack progressed and determine whether the event may affect operational security. Centralised logs also support classification because they allow events to be correlated with alert severity, affected systems, known vulnerabilities, attack patterns and indicators of compromise. In the EPES context, this can help operators distinguish between low-level technical anomalies and cyber-attacks that may have a potential impact on electricity system operation or cross-border electricity flows. In addition, retained SIEM logs and reports can support documentation of the cyber-attack, including the timeline, affected assets, detected indicators, response actions and lessons learned. This documentation is important for internal incident handling, communication with competent authorities or CSIRTs, and post-incident review. Therefore, we agree that centralised logs can support the capabilities described in Article 39(1). However, they should be considered an enabling capability rather than the complete process. Full alignment also requires defined procedures for identifying, classifying, escalating and responding to cyber-attacks, including operational impact assessment and coordination with relevant external actors where required.

KER 10: Chatbot

- *Question: Do you agree that the Chatbot feature of improving the monitoring-driven risk picture could support policies on risk analysis and information system security, as laid out in Article 21(2)(a) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all- hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

- | | |
|-----|---|
| (a) | <i>policies on risk analysis and information system security;</i> |
|-----|---|



Answer: Agree. We agree that the chatbot has the potential to support policies on risk analysis and information system security by improving access to monitoring information and contributing to a more comprehensive operational picture. In the current project, one deployment integrated cybersecurity related data from the IDS through the Intelligent Platform API, allowing operators to query and review relevant information. However, the chatbot does not itself conduct risk assessments, implement security controls, or manage security policies. Its contribution is therefore indirect, supporting operators' awareness and information accessibility rather than replacing formal risk management processes.

- *Question: Do you agree that the Chatbot feature of a faster, more consistent operational evaluation during monitoring could help minimise incident impact, as laid out in Article 21(1) of NIS2?*

NOTE: Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

Answer: Neutral. The chatbot may contribute to operational awareness by providing a simplified interface to access monitoring information. However, in its current implementation, it mainly allows users to query the status of monitored assets and does not perform incident detection, risk analysis, mitigation, or response orchestration. Therefore, while it can facilitate access to information, its contribution to preventing or minimizing the impact of incidents is currently limited and indirect.

- *Question: Do you agree that the tool's feature of collecting information from energy-provider users could support identifying, classifying and responding to cyber-attacks affecting cross-border flows, as laid out in Article 39(1) of the NCCS?*

NOTE: Critical-impact and high-impact entities shall develop the necessary capabilities to handle detected cyber-attacks with the necessary support from the relevant competent authority, the ENTSO for Electricity and the EU DSO entity. The critical-impact and high-impact entities may be supported by the CSIRT designated in their respective Member State as part of the task assigned to the CSIRTs by Article 11(5), point (a) of Directive (EU) 2022/2555. Critical-impact and high-impact entities shall implement effective processes to identify, classify and respond to cyber-attacks that will or may affect cross-border electricity flows in order to minimise their impact.

Answer: Agree. A-Bot chatbot supports Article 39 (1) processes as an enabler of situational awareness: it provides grid operators with a conversational interface to query alerts generated by the IDS on monitored substations, lowering the friction of accessing security information. The detection and classification of cyber-attacks is performed upstream by the IDS, while A-Bot chatbot acts as the conversational layer that delivers this information to the operator. By improving operator responsiveness, A-Bot indirectly



contributes to limiting the propagation of incidents that may affect cross-border electricity flows.

- *Question: Do you agree that the feature of providing aggregated grid-status information could support the CSOC capability to analyse and take protective action, as laid out in Article 38(1) (a)(iii) of the NCCS?*

NOTE: Each high-impact and critical-impact entity shall:

(a) establish, for all assets within its cybersecurity perimeter determined pursuant to Article 26(4) point (c), at least the CSOC capabilities to:

(iii) analyse and, if necessary, take all actions required under its responsibility and capacity to protect the entity;

Answer: Agree. A-Bot chatbot supports the CSOC analysis capability described in Article 38 (1) (a) (iii) by providing operators with a natural-language access to alert information generated by the IDS, lowering the friction of consulting security data during the analysis phase. Autonomous threat analysis and protective actions remain under the responsibility of the CSOC analysts and of the broader detection and response infrastructure; A-Bot contributes by improving the accessibility of the information needed for human decision-making.

KER 11: Guide of recommendations for the safe design of substations

- *Question: Do you agree that the secure-by-design substation guidelines could support security in acquisition/development/maintenance including vulnerability handling, as laid out in Article 21(2)(e) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all- hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

Answer: Agree. Electrical substations are fully affected by NIS2, as relevant assets for the energy industry, targeted by the standard. eFORT has analysis practical implications of security-related goals such as incident monitoring, secure information handling and adapted vulnerabilities and risks

- *Question: Do you agree that the guidelines could support policies on risk analysis and information system security by standardising how design teams address security risks, as laid out in Article 21(2)(a) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all- hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

Answer: Neutral. There exist content in the project results that can be leveraged for that, but an adaption to a common risk methodology analysis would be needed. It is feasible, in any case.



- *Question: Do you agree that the testbook's checklists and tests could support assessing the effectiveness of cybersecurity risk-management measures, as laid out in Article 21(2)(f) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

- (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;*

Answer: Agree. It can be used as a direct verification of measurements in place.

- *Question: Do you agree that the testbook checklists and results could serve as evidence of implementation for audits and supervision, as laid out in Article 32(2)(e) to (g) and 33(2)(d) to (f) of NIS2?*

NOTE: 32(2). Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to:

(e) requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;

(f) requests to access data, documents and information necessary to carry out their supervisory tasks;

(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits

carried out by a qualified auditor and the respective underlying evidence.

33(2). Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to:

(d) requests for information necessary to assess, ex post, the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;

(e) requests to access data, documents and information necessary to carry out their supervisory tasks;

(f) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out.

Answer: Agree. Such testbooks contribute to 2g, 2d and 2f

- *Question: Do you agree that the guide could help implement the minimum and advanced cybersecurity controls for high/critical-impact entities, as laid out in Article 28(2) to (3) and 29(6) of the NCCS?*

NOTE: Article 28:

2. All high-impact entities shall apply the minimum cybersecurity controls pursuant to paragraph 1 point (a) within their high-impact perimeter.



3. All critical-impact entities shall apply the advanced cybersecurity controls pursuant to paragraph 1 point (b) within their critical-impact perimeter.

Article 29(6): Within 12 months after the approval of the minimum and advanced cybersecurity controls pursuant to

Article 8(5), or after each update pursuant to Article 8(10), the entities listed in Article 2(1) and identified as critical-impact and high-impact entities pursuant to Article 24 shall, during the establishment of the entity-level risk mitigation plan pursuant to Article 26(5), apply the minimum cybersecurity controls within the high-impact perimeter and advanced cybersecurity controls within the critical-impact perimeter.

Answer: Agree. eFORT results can contribute to identify risks for enabling an OT-adapted risk-vulnerability workflow

- Question: Do you agree that the guide could be used as input for the cybersecurity procurement recommendations, as laid out in Article 35 of the NCCS?

NOTE: 1. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall develop, in a work programme to be established and updated each time a regional cybersecurity risk assessment report is adopted, sets of non-binding cybersecurity procurement recommendations that high-impact and critical-impact entities may use as a basis for the procurement of ICT products, ICT services and ICT processes in the high-impact and critical-impact perimeters. This work programme shall include the following:

(a) a description and classification of the types of ICT products, ICT services and ICT processes used by high-impact and critical-impact entities in the high-impact and critical-impact perimeter;

(b) a list of the types of ICT products, ICT services, and ICT processes for which a set of non-binding cybersecurity recommendations shall be developed based on the relevant regional cybersecurity risk assessment reports and on the priorities of high-impact and critical-impact entities.

2. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall, within 6 months after the adoption or update of the regional cybersecurity risk assessment report provide ACER with a summary of that work programme.

3. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall endeavour to ensure that the non-binding cybersecurity procurement recommendations developed based on the relevant regional cybersecurity risk assessment are similar or comparable across system operation regions. The sets of cybersecurity procurement recommendations shall cover at least the specifications referred to in Article 33(2), point (a). Where possible, the specifications shall be selected from European and international standards.

4. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall ensure that the sets of cybersecurity procurement recommendations:

(a) comply with the principles of procurement pursuant to Directive 2014/24/EU; and

(b) are compatible with and take into account the most recent available European cybersecurity certification schemes relevant to the ICT product, ICT service, or ICT process.

Answer: Disagree. eFORT results not really oriented to procurement.



- *Question: Do you agree that the guide could serve as documented guidance within the cybersecurity management system, as laid out in Article 32(1)(d), (i) and (l) of the NCCS?*

NOTE: Within 24 months after being notified by the competent authority that they have been identified as a high-

impact or critical-impact entity in accordance with Article 24(6), each high-impact and critical-impact entity shall establish a cybersecurity management system, and review it every three years thereafter, to:

(d) establish a cybersecurity policy that shall be documented and communicated within the entity and to parties affected by the security risks;

(i) create, update and control documented information related to the cybersecurity management system;

(l) review the implementation of the cybersecurity management system at planned intervals; and control and correct non-compliance of the resources and activities with the policies, procedures, guidelines in the cybersecurity management system.

Answer: Disagree. eFORT results not really oriented to management systems.

- *Question: Do you agree that the testbook could supports internal audits and performance/effectiveness evaluation under the cybersecurity management system, as laid out in Article 32(1)(j) to (k) of the NCCS?*

NOTE: Within 24 months after being notified by the competent authority that they have been identified as a high-

impact or critical-impact entity in accordance with Article 24(6), each high-impact and critical-impact entity shall establish a cybersecurity management system, and review it every three years thereafter, to:

(j) evaluate the performance and effectiveness of the cybersecurity management system;

(k) conduct internal audits at planned intervals to ensure that the cybersecurity management system is effectively implemented and maintained;

Answer: Neutral. eFORT results not really oriented to regular audit.

- *Question: Do you agree that secure-by-design substations could be an incident-prevention measure, as laid out in Article 13(1)(a) of CER?*

NOTE: Member States shall ensure that critical entities take appropriate and proportionate technical, security and

organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

- (a) prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures.*

Answer: Agree. Risk findings and SoA, as well as specific results related to this one, include solutions designed for intrusion detection.

- *Question: Do you agree that the design guidelines could operationalise adequate physical protection at substation level, as laid out in Article 13(1)(b) of CER?*



NOTE: Member States shall ensure that critical entities take appropriate and proportionate technical, security and

organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

(b) ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls

Answer: Disagree. eFORT results in this KER not oriented to physical protection.

- *Question: Do you agree that the guide could support responding to, resisting and mitigating the consequences of incidents through early malfunction detection, as laid out in Article 13(1)(c) of CER?*

NOTE: Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

(c) respond to, resist and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;

Answer: Strongly agree. Risk findings and SoA, as well as specific results related to this one, include solutions designed for intrusion detection and alarm generation.

KER 12: RTU

- *Question: Do you agree that the RTU's data feed, by enabling earlier visibility through monitoring, could help minimise the impact of incidents on recipients of services, as laid out in Article 21(1) of NIS2?*

NOTE: Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

Answer: Agree. Early visibility from RTU monitoring enables faster incident response and mitigation, reducing impact on services in line with NIS2 Article 21(1).

- *Question: Do you agree that the RTU's trigger-on-change and trigger-on-quality reporting could supply signals that could feed the identification and classification of cyber-attacks, as laid out in Article 39(1) of the NCCS?*

NOTE: Critical-impact and high-impact entities shall develop the necessary capabilities to handle detected cyber-attacks with the necessary support from the relevant competent authority, the ENTSO for Electricity and the EU DSO entity. The critical-impact and high-impact entities may be



supported by the CSIRT designated in their respective Member State as part of the task assigned to the CSIRTs by Article 11(5), point (a) of Directive (EU) 2022/2555. Critical-impact and high-impact entities shall implement effective processes to identify, classify and respond to cyber-attacks that will or may affect cross-border electricity flows in order to minimise their impact.

Answer: Agree. Do you agree that the RTU's trigger-on-change and trigger-on-quality reporting could supply signals that could feed the identification and classification of cyber-attacks, as laid out in Article 39(1) of the NCCS?

KER 13: Blockchain for grid resiliency

- *Question: Do you agree that the blockchain feature of supply-chain tracing of energy facility components could support supply chain security with direct suppliers and service providers, as laid out in Article 21(2)(d) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all- hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

Answer: Agree. Blockchain-based tracing can support supply chain security by creating a tamper-evident record of component origin, ownership, handling, and supplier involvement. However, it should complement supplier due diligence, contractual controls, verification, and security testing rather than replace them.

- *Question: Do you agree that the traceability of the tool could support considering supplier-specific vulnerabilities and the quality of suppliers' products and cybersecurity practices, as laid out in Article 21(3) of NIS2?*

NOTE: Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

Answer: Agree. Traceability can help link components, suppliers, service providers, and lifecycle events, making it easier to assess supplier-specific risks, vulnerabilities, and product quality. However, cybersecurity practices still need to be verified through audits, certifications, testing, and contractual requirements.

- *Question: Do you agree that monitoring energy consumption at TSO level could support policies on risk analysis and information system security by detecting abnormal patterns, as laid out in Article 21(2)(a) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all- hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security.



Answer: Agree. Monitoring energy consumption at TSO level can help detect abnormal patterns that may indicate cyber incidents, manipulation, or operational anomalies. However, it should complement broader risk analysis, cybersecurity monitoring, and information system security policies rather than replace them.

- *Question: Do you agree that consumption monitoring could support incident handling, as laid out in Article 21(2)(b) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(b) incident handling;

Answer: Agree. Consumption monitoring can help identify abnormal demand patterns, support incident triage, and provide evidence for assessing the scope and impact of an incident. However, it should be combined with cybersecurity logs, operational data, and incident-response procedures.

- *Question: Do you agree that blockchain traceability could support the traceability and audit-evidence aspects of the minimum and advanced cybersecurity controls in the supply chain, as laid out in Article 33(2)(a)(vii) to (x) of the NCCS?*

NOTE: 2. The minimum cybersecurity controls in the supply chain shall consist of controls for high-impact and critical-impact entities that:

(a) include recommendations for the procurement of ICT products, ICT services, and ICT processes referring to cybersecurity specifications, covering at least:

(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;

(viii) the support for security updates throughout the entire lifetime of ICT products, ICT services or ICT processes;

(ix) the right to audit cybersecurity in the design, development and production processes of the supplier; and

(x) the assessment of the risk profile of the supplier;

Answer: Agree. Blockchain traceability can provide tamper-evident records across development, production, delivery, updates, and supplier actions, supporting traceability and audit evidence. However, it does not replace supplier audits, risk assessments, update obligations, or contractual cybersecurity requirements.

- *Question: Do you agree that the tool's consumption anomaly signals could support identifying, classifying and responding to cyber-attacks affecting cross-border flows, as laid out in Article 39(1) of the NCCS?*

NOTE: Critical-impact and high-impact entities shall develop the necessary capabilities to handle detected cyber-attacks with the necessary support from the relevant competent authority, the ENTSO for Electricity and the EU DSO entity. The critical-impact and high-impact entities may be supported by the CSIRT designated in their respective Member State as part of the task assigned to the CSIRTs by Article 11(5), point (a) of Directive (EU) 2022/2555. Critical-impact and high-impact entities shall implement effective processes to identify, classify and respond to cyber-attacks that will or may affect cross-border electricity flows in order to minimise their impact.



Answer: Agree. Consumption anomaly signals can help identify unusual operational patterns that may indicate cyber-attacks affecting electricity flows, and can support classification and response decisions. However, they should be correlated with grid telemetry, cybersecurity logs, and operational analysis before concluding that an anomaly is cyber-related.

- *Question: Do you agree that supply-chain traceability could support the alternative supply chains measure, as laid out in Article 13(1)(d) of CER?*

NOTE: Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

(d) recover from incidents, duly considering business continuity measures and the identification of alternative supply chains, in order to resume the provision of the essential service;

Answer: Agree. Supply-chain traceability can help identify component origins, supplier dependencies, and potential alternative suppliers, supporting business continuity and recovery planning. However, it does not by itself ensure alternative supply chains are available; this also requires procurement planning, supplier qualification, contracts, and resilience testing.

- *Question: Do you agree that TSO consumption monitoring could support preventing incidents and responding to, resisting and mitigating their consequences, as laid out in Article 13(1)(a) and (c) of CER?*

NOTE: Member States shall ensure that critical entities take appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:

(a) prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;

(c) respond to, resist and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;

Answer: Agree. TSO consumption monitoring can help detect abnormal patterns early, support alert routines, and inform operational response to prevent or mitigate incidents. However, it should be combined with risk management procedures, crisis protocols, cybersecurity monitoring, and resilience planning.

KER 14: SOAR

- *Question: Do you agree that the tool's incident-handling automation could support incident handling, as laid out in Article 21(2)(b) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(b) incident handling.

Answer: Strongly agree. This is the automation of incident handling, so completely in line with each other.



- *Question: Do you agree that the tool's faster, repeatable response could reduce incident impact on service recipients, as laid out in Article 21(1) of NIS2?*

NOTE: Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

Answer: Strongly agree. Faster response can reduce impact.

- *Question: Do you agree that SOAR playbooks and automated response could support the CSOC capability to analyse and take protective action for the entity, as laid out in Article 38(1)(a)(iii) of the NCCS?*

NOTE: Each high-impact and critical-impact entity shall:

(a) establish, for all assets within its cybersecurity perimeter determined pursuant to Article 26(4) point (c), at least the CSOC capabilities to:

(iii) analyse and, if necessary, take all actions required under its responsibility and capacity to protect the entity;

Answer: Strongly agree. This is the automation of incident handling, so completely in line with each other.

KER 15: Blueprint for EPES SOC infrastructure

- *Question: Do you agree that the SOC blueprint could help establish and standardise incident-handling capability, as laid out in Article 21(2)(b) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(b) incident handling;

Answer: Strongly agree. This is the automation of incident handling, so completely in line with each other.

- *Question: Do you agree that faster, more consistent SOC stand-up could help minimise incident impact, as laid out in Article 21(1) of NIS2?*

NOTE: Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-art and, where



applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

Answer: Strongly agree. Automated and faster response can reduce impact of an attack.

- *Question: Do you agree that the blueprint could be a concrete reference design for establishing CSOC capabilities, as laid out in Article 38(1)(a)(i) to (iv) of the NCCS?*

NOTE: Each high-impact and critical-impact entity shall:

(a) establish, for all assets within its cybersecurity perimeter determined pursuant to Article 26(4) point (c), at least the CSOC capabilities to:

(i) ensure that the relevant network and information systems and applications provide security logs for security monitoring to enable the detection of anomalies and collect information on cyber-attacks;

Answer: Strongly agree. This is the automation of incident handling, so completely in line with each other.

- *Question: Do you agree that the blueprint could define the processes, roles and information flows needed to share reportable cyber-attack information within 4 hours, as laid out in Article 38(3) of the NCCS?*

NOTE: Each critical-impact and high-impact entity shall share relevant information related to a reportable cyber-attack with its CSIRTs and its competent authority without undue delay and no later than four hours of becoming aware that the incident is reportable.

Answer: Strongly agree. The blueprint includes playbook sharing.

KER 21: Connected devices vulnerabilities

- *Question: Do you agree that identifying device vulnerabilities could support vulnerability handling and disclosure, as laid out in Article 21(2)(e) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

Answer: Strongly agree. Absolutely. First, you have to identify the vulnerability so that you can start a responsible vulnerability disclosure procedure and handling the vulnerability (e.g., providing a patch).

- *Question: If the tool includes coordinated disclosure, do you agree that the tool could help align with the coordinated vulnerability disclosure framework and the European vulnerability database, as laid out in Article 12(1) and 12(2) of NIS2?*



NOTE: 1. Each Member State shall designate one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure. The CSIRT designated as coordinator shall act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party. The tasks of the CSIRT designated as coordinator shall include:

- (a) identifying and contacting the entities concerned;*
- (b) assisting the natural or legal persons reporting a vulnerability; and*
- (c) negotiating disclosure timelines and managing vulnerabilities that affect multiple entities.*

Member States shall ensure that natural or legal persons are able to report, anonymously where they so request, a vulnerability to the CSIRT designated as coordinator. The CSIRT designated as coordinator shall ensure that diligent follow-up action is carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability. Where a reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT designated as coordinator of each Member State concerned shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.

2. ENISA shall develop and maintain, after consulting the Cooperation Group, a European vulnerability database. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures, and shall adopt the necessary technical and organisational measures to ensure the security and integrity of the European vulnerability database, with a view in particular to enabling entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, to disclose and register, on a voluntary basis, publicly known vulnerabilities in ICT products or ICT services. All stakeholders shall be provided access to the information about the vulnerabilities contained in the European vulnerability database. That database shall include:

- (a) information describing the vulnerability;*
- (b) the affected ICT products or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited;*
- (c) the availability of related patches and, in the absence of available patches, guidance provided by the competent authorities or the CSIRTs addressed to users of vulnerable ICT products and ICT services as to how the risks resulting from disclosed vulnerabilities can be mitigated.*

Answer: Neutral. The tool does not cover the disclosure part.

- **Question:** *Do you agree that the tool could support supply chain security, as laid out in Article 21(2)(d) of NIS2?*

NOTE: The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

- (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;*

Answer: Agree. The vulnerabilities found in IoT devices in T2.2 could be reported and considered in supply chain security.



- *Question: Do you agree that the tool could support entities to consider supplier-specific vulnerabilities and suppliers' cybersecurity practices, as laid out in Article 21(3) of NIS2?*

NOTE: Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

Answer: Agree. The vulnerabilities found in IoT devices in T2.2 could be reported and considered in supply chain security.

- *Question: Do you agree that discovered vulnerabilities could be inputs to the entity-level cybersecurity risk assessment, as laid out in Article 26(4)(a)(i) to (vi) of the NCCS?*

NOTE: During the cybersecurity risk assessment phase, each high-impact and critical-impact entity shall:

(a) identify cybersecurity risks by taking into account:

(i) all assets supporting the Union-wide high-impact and critical-impact processes with an assessment of the possible impact on cross-border electricity flows if the asset is compromised;

(ii) possible cyber threats taking into account the cyber threats identified in the latest Comprehensive cross-border electricity cybersecurity risk assessment report referred to in Article 23 and supply chain threats;

(iii) vulnerabilities, including vulnerabilities in legacy systems;

(iv) possible cyber-attack scenarios, including cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows;

(v) relevant risk evaluations and assessments carried out at Union level, including coordinated risk assessments of critical supply chains in accordance with Article 22 of Directive (EU) 2022/2555; and

(vi) existing implemented controls;

Answer: Agree. The vulnerabilities found in IoT devices in T2.2 could be reported and considered in supply chain security.

- *Question: Do you agree that the findings could support selecting risk treatment options and determining residual risk, as laid out in Article 26(5) to (6) of the NCCS?*

NOTE: During the cybersecurity risk treatment phase, each high-impact and critical-impact entity shall establish an

entity-level risk mitigation plan by selecting risk treatment options appropriate to manage the risks and identify the residual risks.

6. During the cybersecurity risk acceptance phase, each high-impact and critical-impact entity shall decide



whether to accept the residual risk based on the risk acceptance criteria established in paragraph 3 point (b).

Answer: Agree. Vulnerabilities can be assigned CVSS to indicate how critical they are. This information can be considered for risk assessment.

- *Question: Do you agree that an actively exploited, unpatched in-scope vulnerability could form the relevant information notified to the CSIRT, as laid out in Article 38(5) of the NCCS?*

NOTE: Where critical-impact and high-impact entities notify relevant information related to unpatched actively exploited vulnerabilities to a CSIRT, the latter may forward this information to its competent authority. In light of the level of sensitivity of the notified information, the CSIRT may withhold the information or delay its forwarding based on justified cybersecurity-related grounds.

Answer: Agree. Same reason as in 17.

- *Question: Do you agree that the findings could support manufacturers' vulnerability-handling obligations, as laid out in Article 6(b) and Annex I, Part II, points 1 to 8 of the CRA?*

NOTE: Products with digital elements shall be made available on the market only where:

(c) the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I.

Part II Vulnerability handling requirements

Manufacturers of products with digital elements shall:

- (1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;*
- (2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;*
- (3) apply effective and regular tests and reviews of the security of the product with digital elements;*
- (4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;*
- (5) put in place and enforce a policy on coordinated vulnerability disclosure;*
- (6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;*



(7) *provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;*

(8) *ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.*

Answer: Agree. As a result of the responsible vulnerability disclosure the manufacturer should handle the vulnerability.

- *Question: Do you agree that, for devices with operational or physical-service impact, the vulnerability findings could support the critical-entity risk assessment, as laid out in Article 12(1) and 12(2) of CER?*

NOTE: 1. Notwithstanding the deadline set out in Article 6(3), second subparagraph, Member States shall ensure that critical entities carry out a risk assessment within nine months of receiving the notification referred to in Article 6(3), whenever necessary subsequently, and at least every four years, on the basis of Member State risk assessments and other relevant sources of information, in order to assess all relevant risks that could disrupt the provision of their essential services ('critical entity risk assessment').

2. Critical entity risk assessments shall account for all the relevant natural and man-made risks which could lead to an incident, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats and other antagonistic threats, including terrorist offences as provided for in Directive (EU) 2017/541. A critical entity risk assessment shall take into account the extent to which other sectors as set out in the Annex depend on the essential service provided by the critical entity and the extent to which that critical entity depends on essential services provided by other entities in such other sectors, including, where relevant, in neighbouring Member States and third countries.

Answer: Agree. Same reason as in previous question related to risk assessment.



ANNEX IV Results survey on IEC 62443

As part of the analysis conducted in Task 6.5, a survey was distributed to the relevant task leaders to evaluate cybersecurity standards and communication protocol challenges in a real environment,

The survey was structured according to the different KERs. For each KER, respondents were asked to answer a set of questions using the same five-point scale: Strongly agree, Agree, Neutral, Disagree, or Strongly disagree. After each question, respondents were also asked to briefly explain the reasoning behind their chosen answer. To avoid repetition, these response options and the request for explanation are not repeated for every individual question. The following paragraphs present the structure of the survey and the results.

Personal information

- What is your full name?
- For which eFORT partner company do you work?
- What eFORT task are you working on?
- Which KER is relevant to you?

KER 1: eFORT Intelligent Platform

- *Question: Do you agree that the Integrated tools for threat prevention, detection, monitoring, visualization, grid adaptation and collaborative response can support: IEC 62443-3-3 system security requirements for monitoring, detection and event handling AND/OR IEC 62443-3-2 risk-based system architecture. Please explain your answer choice.*

Answer 1: Agree. Authentication, RBAC, and secure session management. Input data validation to prevent SQL injection or XSS. Encryption in transit (HTTPS) and at rest (encryption of credentials and API tokens). Use of secure APIs. Security logs and request traceability.

Answer 2: Agree. The eFORT Intelligent Platform supports these IEC 62443 objectives by enabling secure data collection, monitoring, anomaly detection, alert generation and event visualisation. It also contributes to a risk-based architecture by integrating cybersecurity and risk-related information from different tools. However, it should be considered a supporting component within a broader IEC 62443-compliant architecture, not a standalone guarantee of full compliance.

KER 2: Data Base Tool

- *Question: Do you agree that the visualization and monitoring of EPES security state using static and dynamic vulnerability data can support: IEC 62443-3-2 requirements for asset identification, vulnerability identification and risk assessment AND/OR IEC 62443-2-1 security management processes. Please explain your answer choice.*



Answer: Agree. The visualization and monitoring of the EPES security state using both static and dynamic vulnerability data can support IEC 62443-3-2 requirements for asset identification, vulnerability identification and risk assessment, as well as IEC 62443-2-1 security management processes. For IEC 62443-3-2, the support is direct. The Vulnerabilities Database tool provides an asset-oriented vulnerability knowledge base: it aggregates known vulnerability sources, removes duplicates, classifies vulnerabilities by asset type and infrastructure category, and requires asset registration/profile information such as asset type and operating system. This creates a structured basis for identifying which EPES assets may be exposed to known weaknesses. In addition, the dynamic risk assessment approach enriches asset data with public vulnerability sources and estimates risk based on asset exposure, vulnerability criticality and potential impact on the power infrastructure. This is highly relevant to the IEC 62443-3-2 risk-assessment logic, where the organisation must understand the system under consideration, identify assets, identify threats and vulnerabilities, and assess risk.

KER 3: Secure Box

- *Question: Do you agree that the secure Box as an embedded device for real-time cyber protection of local areas such as microgrids and substations can support: IEC 62443-4-2 component security requirements AND/OR IEC 62443-3-3 boundary protection and integrity requirements. Please explain your answer choice.*

Answer: Strongly agree. SecureBox could support IEC 62443-4-2 because the itself implements secure component features such as access control, hardening, integrity protection, and secure communications. It can also support IEC 62443-3-3 by helping enforce local boundary protection and integrity monitoring in substations or microgrids.

KER 4: Training through CRoF and digital twin of the power grids

- *Question. Do you agree that real-time digital twin for attack simulation, impact analysis and cyber-security training can support: IEC 62443-2-1 requirements for competence, training and awareness AND/OR IEC 62443-3-2 risk understanding. Please explain your answer choice.*

Answer: Strongly agree. Real-time digital twins provide a realistic and safe environment for simulating cyberattacks. It can help with analyzing the impact, and training personnel. This improves cybersecurity awareness, competence, and risk understanding, which directly supports the objectives of IEC 62443-2-1 and IEC 62443-3-2.

KER 5: Dynamic Risk Assessment Tools

- *Question: Do you agree that the Geo-referred risk assessment tool and the Dynamic risk assessment methodology can support: IEC 62443-3-2 zone, conduit and risk assessment requirements. Please explain your answer choice.*



Answer: Strongly disagree. The Geo-referred risk assessment tool as well as the Dynamic risk assessment methodology focus on physical threats and physical effect modelling/assessment, respectively.

KER 6: IDS

- *Question: Do you agree that detection of suspicious actions in networks and equipment using host and network-based IDS with AI algorithms can support: IEC 62443-3-3 related to detection of security events and system integrity monitoring. Please explain your answer choice.*

Answer: Agree. A host and network-based IDS can support security-event detection and system integrity monitoring by identifying suspicious activity in substation networks and equipment. AI algorithms may improve anomaly detection, but they should be validated and complemented by rules, logging, and incident-response procedures.

KER 7: SIEM

- *Question: Do you agree that Cloud-based log collection, storage and correlation software can support: IEC 62443-3-3 monitoring and IEC 62443-2-1 security operations and incident management. Please explain your answer choice.*

Answer: Agree. For KER 9 / SIEM, the support is complementary and operational. The eSIEM collects logs, network traffic, IDS findings and security alerts from IT and OT components, including power-grid-specific assets such as SCADA systems, PLCs, RTUs, protection relays and other infrastructure nodes. It also correlates heterogeneous data sources, provides topology views, node hygiene/health scores, vulnerability-related information, MITRE ATT&CK mappings and alert dashboards. This turns the static vulnerability baseline into a monitored, continuously updated view of the EPES security state. The SIEM also interfaces with the Vulnerability Database to identify potentially vulnerable services and assets, which strengthens both vulnerability identification and risk prioritisation. For IEC 62443-2-1, the tools support the implementation of cybersecurity management processes, but they do not replace the need for formal organisational procedures. IEC 62443 as a series is intended to define requirements and processes for implementing and maintaining secure industrial automation and control systems, including both technical and organisational aspects. The Vulnerabilities Database and SIEM can provide evidence and operational support for processes such as asset inventory maintenance, vulnerability management, continuous monitoring, incident detection, mitigation planning, auditability and security posture reporting. However, full IEC 62443-2-1 alignment would also require documented governance, roles and responsibilities, risk acceptance criteria, remediation workflows, periodic review, and integration into the asset owner's cybersecurity management system. The same logic is also relevant for EU regulatory expectations. For example, NIS2 places emphasis on cybersecurity risk-management measures and incident reporting obligations, while the Cyber Resilience Act establishes cybersecurity and vulnerability-handling requirements for products with digital elements. Therefore, these tools can provide useful technical evidence and monitoring capabilities to support compliance-



oriented cybersecurity management in EPES environments, although they should be considered enabling tools rather than a complete compliance solution by themselves.

KER 8: Chatbot

- *Question: Do you agree that interactive interface providing aggregated grid security information to operators can support: IEC 62443-2-1 operational processes and incident response support. Please explain your answer choice.*

Answer: Agree. We agree that such an interface can support IEC 62443-2-1 operational processes by improving operator access to relevant monitoring information. In the current project, one deployment integrates cybersecurity-related data from an IDS through an API from the Intelligent Platform, enabling operators to query this information through a conversational interface. While the chatbot is not directly integrated into incident response workflows and its notification mechanism has not yet been adopted, it can contribute to situational awareness and facilitate access to information that may assist operators during the analysis of security related events.

KER 9: Guide of recommendations for the safe design of substations

- *Question: Do you agree that Security guidelines and testbooks for secure substation design and assessment can support: IEC 62443-3-2 secure architecture AND/OR IEC 62443-2-1 policies and procedures. Please explain your answer choice.*

Answer: Answer not provided.

KER 10: RTU

- *Question: Do you agree that improved functionalities for RTUs used as substation device can support: IEC 62443-4-2 component security requirements for field and control devices. Please explain your answer choice.*

Answer: Agree. Enhanced RTU functionalities improve cybersecurity at device level, helping meet IEC 62443-4-2 requirements for secure field and control systems.

KER 11: Blockchain for grid resiliency

- *Question: Do you agree that Blockchain for supply-chain traceability and energy consumption monitoring can support: IEC 62443-3-3 integrity and availability objectives. Please explain your answer choice.*

Answer: Agree. Blockchain can support integrity by providing tamper-evident records for supply-chain data and energy-consumption events. It may also support availability indirectly by improving traceability and anomaly visibility, but it does not by itself ensure system availability or operational resilience.



KER 12: SOAR

- *Question: Do you agree that Open-source orchestration and automation of SOC security workflow can support: IEC 62443-2-1 incident response processes AND/OR IEC 62443-3-3 monitoring. Please explain your answer choice.*

Answer 1: Agree. Agree, provided that open-source orchestration solutions meet strict security, reliability, and IEC 62443 compliance requirements, and can be safely integrated into TenneT's critical OT/IT environment.

Answer 2: Agree. In the IT/OT combined response, it is important to interface with standards both in the IT and OT domain

KER 13: Blueprint for EPES SOC infrastructure

- *Question: Do you agree that reference SOC architecture for EPES environments can support: IEC 62443-2-1 governance and operational organization requirements. Please explain your answer choice.*

Answer 1: Agree. The SOC architecture needs to be integrated in the EPES environment, which is designed with the IEC 62443-2-1 in mind

Answer 2: Neutral. We have not been involved in the definition of the reference SOC architecture for EPES of eFORT, so we do not have an opinion on the matter.

KER 14: Connected devices vulnerabilities

- *Question: Do you agree that identification of vulnerabilities in connected devices can support: IEC 62443-3-2 asset identification AND/OR IEC 62443-2-3 vulnerability and patch management. Please explain your answer choice.*

Answer : Answer not provided.



ANNEX V Relevant OT Communication Protocols

Deterministic Ethernet. Refers to a set of technologies and standards that extend traditional Ethernet to guarantee predictable, time-bounded data delivery, which is essential for real-time and mission-critical applications. Unlike standard Ethernet, where packet delivery can be delayed due to congestion or collisions, deterministic Ethernet uses mechanisms such as time synchronization, traffic scheduling, and prioritization to ensure low latency, minimal jitter, and high reliability. These capabilities make it especially suitable for industrial automation, automotive networks, aerospace systems, and other environments where precise timing and consistent communication are required. Standards such as Time-Sensitive Networking (TSN) play a key role in enabling deterministic behavior while maintaining compatibility with conventional. See Table 7-2 for comparison against FR 1-7.

Deterministic Ethernet is mainly on layer 2 in the ISO/OSI stack and thus delegates a number of security functions to higher levels. It does provide some availability – thus being helpful for FR7 (resource availability) and FR6 (Timely Response to Events), as well as being useable for network segregation (FR5). It does assume non-malicious devices, which means that a malicious actor with a compromised deterministic ethernet protocol can still upset the network and negate those effects.

Deterministic Ethernet Summary. Deterministic Ethernet does not claim to offer significant security, so the corresponding responsibility is on other, higher-level protocols. It does offer some attack surface itself (e.g., disrupting the scheduling mechanism), which cannot be addressed on a higher level, and that would disrupt the timing guarantees this protocol is giving.

Mitigation: Defending against a rogue device that is disrupting the schedule is hard; this makes it important to harden devices so they cannot easily be compromised, and to perform monitoring on the network to detect malicious communication disruptions.

Deterministic Ethernet can be flanked by MACsec, which adds a security layer on OSI layer 2. MACsec offers authentication and (optionally) encryption. This is done on a hop-to-hop basis, i.e., MACsec cannot deliver end-to-end security. It also supports different channels, i.e., can cryptographically separate communication links on the same network. MACsec itself does not handle key management, but a companion standard exists (IEEE 802.1X-2010), that defines MKA (MACsec Key Agreement) and offers certificate based key management for MACsec devices.

In this, MACsec + MKA does help with a number of security requirements on the level where it can; some issues cannot be resolved on the MAC layer, so higher level protocols are not absolved.

Table 7-2. Foundational Requirements FR1-7 - Deterministic Ethernet with MACsec and MKA assessment.

Foundational Requirement	Deterministic Ethernet with MACsec and MKA
FR1: Identification	Good at the link level when MKA is used: devices participating in a MACsec connectivity association can be authenticated before protected traffic is



Foundational Requirement	Deterministic Ethernet with MACsec and MKA
and Authentication	exchanged. This authenticates network attachment, not application users or OT roles.
FR2: Use Control	Limited. MACsec can restrict which devices may join a protected Layer 2 segment, but it does not provide command-level authorization, user roles, or least-privilege control for OT operations.
FR3: System Integrity	Good at the link level: MACsec provides frame integrity, origin authenticity within the secured link, and replay protection. It does not protect data once it leaves the protected Layer 2 hop or after decryption at intermediate devices.
FR4: Data Confidentiality	Good at the link level when encryption is enabled. Confidentiality is hop-by-hop rather than end-to-end, so higher-layer protection is still required where traffic crosses gateways, routed networks, or untrusted systems.
FR5: Restricted Data Flow	Moderate. MACsec can support secure Layer 2 segmentation and cryptographic separation of connectivity associations, but zoning, conduits, routing policy, and application-level filtering remain architectural controls.
FR6: Timely Response to Events	Limited. Authentication or integrity failures may be observable by network infrastructure, but MACsec itself does not provide OT-aware security event semantics, audit trails, or application-level alarms.
FR7: Resource Availability	Limited to moderate. MACsec can prevent unauthorised devices from injecting valid protected traffic, but it does not by itself prevent physical-layer disruption, link flooding, scheduling disruption, or denial-of-service by an already authorised or compromised device.

CAN bus. CAN bus (Controller Area Network) is a real-time serial communication protocol originally developed for automotive systems and now widely used in industrial automation and embedded control, and seen in the energy sector, for example in BESS. It enables microcontrollers and devices to communicate over a shared bus without a central host, using message-based communication with priority-driven arbitration to ensure deterministic behavior. CAN bus is highly reliable due to built-in error detection, fault confinement, and automatic retransmission, supports high noise immunity in harsh environments, and serves as the foundation for higher-layer protocols, a bit like Ethernet. In this, it shares the security properties with deterministic Ethernet; it adds a layer of robustness to the communication layer but needs higher-level protocols to deploy security measures and requires some protection and monitoring against compromised devices performing a denial-of-service attack.

In the newer CAN XL, a security extension, CANsec, does add message authentication; Integrity protection, optional Encryption, and replay protection. It also introduces “cryptographic zoning”, i.e., different groups of devices have different keys and thus cannot authenticate (or encrypt) traffic from devices outside of their group.



CANsec does not handle key management. This leaves one of the more challenging problems to outside protocols, but also immunizes the protocol from post quantum issues, as it already supports AES 256 and does not use public key cryptography.

CANsec is a comparatively new protocol and thus has not seen much adoption yet; practical issues in its usage are still to be seen, especially in the energy sector. See Table 7-3 for comparison against FR 1-7.

Table 7-3. Foundational Requirements FR1-7 - CANsec assessment.

Foundational Requirement	CANsec
FR1: Identification and Authentication	Moderate at the message-group level. CANsec can authenticate frames within configured cryptographic zones, but it does not provide rich device identity, user identity, or application-level authentication semantics.
FR2: Use Control	Limited. Cryptographic zoning can restrict which device groups can exchange valid protected frames, but CANsec does not provide role-based authorization, command-level permissions, or separation of read, write, and administrative functions.
FR3: System Integrity	Good for protected CAN XL frames: provides message authentication, integrity protection, and replay protection. It does not protect higher-layer application semantics or prevent misuse by an authenticated but compromised device.
FR4: Data Confidentiality	Good when optional encryption is enabled. If encryption is not enabled, CANsec still provides authenticity and integrity but not confidentiality.
FR5: Restricted Data Flow	Moderate. Cryptographic zones can separate groups of communicating devices, but bus-level topology, gateway policy, and higher-layer filtering remain necessary for enforceable OT zoning and conduits.
FR6: Timely Response to Events	Limited. Authentication, integrity, or replay failures may be detectable by implementations, but CANsec does not define a complete logging, alerting, or SOC integration model.
FR7: Resource Availability	Limited. CAN itself provides robust error detection and arbitration, but CANsec does not eliminate denial-of-service risks from bus flooding, malformed traffic, or a compromised authorised device. Availability protection still requires physical protection, bus guardianship, rate limiting, and monitoring.

450Connect. This communication protocol is a German nationwide 450 MHz LTE450 network for utilities and critical infrastructure. It is designed to be a robust backup communication channel for critical infrastructure using the 450MHz band and backed by a consortium of German energy- and water providers. 450Connect is designed to reliably connect distributed systems and thus would be located between Operations and SCADA. It also does not implement security functionality, but is mainly seen as a reliable, protocol agnostic communication medium. To protect the communication medium itself, it does



perform subscriber authentication and utilizes the normal LTE/5G security to protect against outside attacks. There is no protection once a device does obtain network access, though. See Table 7-4 for comparison against FR 1-7.

Table 7-4. Foundational Requirements FR1-7 - 450connect assessment.

Foundational Requirement	450Connect assessment
FR1: Identification and Authentication	Good at the network-access level: LTE subscriber authentication and SIM/eSIM-based identity can restrict access to authorised devices. This does not replace application-layer device, user, or command authentication.
FR2: Use Control	Limited. 450connect can support network access control and separation of customer or service domains, but it does not provide OT command authorization, role-based access control, or least-privilege enforcement for applications.
FR3: System Integrity	Moderate at the cellular bearer level: LTE security mechanisms can protect signalling and user-plane traffic against external radio-access attacks. End-to-end message integrity for SCADA or OT protocols must still be provided by higher-layer protocols.
FR4: Data Confidentiality	Moderate at the bearer level: cellular encryption protects traffic over the radio/network segment, but application-layer confidentiality remains necessary where traffic traverses gateways, enterprise systems, cloud services, or other networks.
FR5: Restricted Data Flow	Moderate to good as a communication bearer. Private APNs, closed network designs, customer separation, routing policy, and service prioritisation can support zoning and conduits, but OT segmentation and protocol-level allow-listing still need to be implemented architecturally.
FR6: Timely Response to Events	Moderate. Network operations can provide availability and connectivity monitoring, but OT security event semantics, command audit trails, and SOC integration depend on the connected applications and operator monitoring architecture.
FR7: Resource Availability	Good as a resilient communication bearer when engineered accordingly: 450 MHz propagation, utility-oriented operation, prioritisation, and blackout-resilience concepts support availability. However, application resilience, endpoint hardening, and fallback operation remain separate system responsibilities.

DNP3. Distributed Network Protocol version 3, standardized as IEEE 1815, is a communication protocol for SCADA and utility automation systems, particularly in electric, water, and gas infrastructure. It is designed event-driven data exchange between control centers and remote field devices over serial or IP-based networks, supporting time-stamped events, unsolicited reporting, and robust error detection. DNP3



uses a layered architecture with efficient bandwidth usage, support for unreliable communication links, and optional security enhancements through DNP3 Secure Authentication (based on IEC 62351) adds a number of integrity protection mechanisms. See Table 7-5 for comparison against FR 1-7.

Table 7-5. Foundational Requirements FR1-7 - DNP3 assessment.

Foundational Requirement	DNP3
FR1: Identification and Authentication	Moderate when DNP3 Secure Authentication is deployed: supports authentication of critical operations and user/accountability mechanisms. Plain DNP3 provides no modern authentication.
FR2: Use Control	Limited. DNP3 Secure Authentication can support user association for critical functions, but fine-grained role-based authorization and least-privilege command control normally depend on the master, outstation, gateway, and operational architecture.
FR3: System Integrity	Good for selected critical operations when Secure Authentication is used: provides message authentication, integrity protection, and replay protection. Plain DNP3 remains vulnerable to spoofing, modification, and replay.
FR4: Data Confidentiality	Weak at the DNP3 application layer. Secure Authentication does not provide payload encryption by itself; confidentiality normally requires TLS, VPN, or another transport/network-layer protection mechanism.
FR5: Restricted Data Flow	Moderate. DNP3 has well-defined master-outstation communication patterns that can support zoning, conduits, allow-listing, and gateway architectures, but it is not itself zone-aware and relies on external network segmentation.
FR6: Timely Response to Events	Moderate. DNP3 supports time-stamped events, event classes, unsolicited reporting, and event buffering, which are useful for operational monitoring. Security event logging and SOC integration depend on implementation and surrounding systems.
FR7: Resource Availability	Moderate operational resilience through event buffering, efficient bandwidth use, error detection, and suitability for unreliable links. However, protocol-level DoS resistance is limited and should be supplemented by rate limiting, segmentation, and monitoring.

IEC 60870-5-104. Often shortened to **IEC 104**, it is a communication protocol used in electric power and industrial automation systems to transmit data between control centers and remote terminal units over standard IP networks. It is essentially the TCP/IP adaptation of IEC 60870-5-101, preserving the same application layer and data models while replacing serial links with Ethernet and TCP for higher speed, longer distance, and easier network integration. IEC 104 supports real-time monitoring and control through standardized information objects (such as measurements, commands, and alarms), uses a client-server model, and is widely deployed in SCADA systems for substations,



grid control, and energy management. It can be seen as the predecessor for 61850. See Table 7-6 Table 7-2 for comparison against FR 1-7.

Table 7-6. Foundational Requirements FR1-7 - IEC 60870-5-104 assessment.

Foundational Requirement	IEC 60870-5-104
FR1: Identification and Authentication	Weak in plain IEC 60870-5-104. Secure operation requires IEC 62351-3 transport security and IEC 62351-5 / IEC TS 60870-5-7 application-layer security to authenticate communication partners and authorised users.
FR2: Use Control	Limited in the base protocol. IEC TS 60870-5-7:2025 adds support for role-based access control using the IEC 62351-8 approach, but practical command-level least privilege depends on implementation and operational configuration.
FR3: System Integrity	Weak in plain IEC 104. IEC 62351-5 and IEC TS 60870-5-7 can provide origin authentication, integrity protection, and replay protection for APDUs and critical operations.
FR4: Data Confidentiality	Not provided by the base protocol. Confidentiality normally requires IEC 62351-3 TLS, VPN, or other secure transport protection, especially where IEC 104 crosses routed or shared networks.
FR5: Restricted Data Flow	Moderate. IEC 104 has predictable master-station and controlled-station communication patterns and well-known ports, which support zoning, conduits, allow-listing, and gateway designs, but the protocol is not itself zone-aware.
FR6: Timely Response to Events	Moderate for operational events because IEC 104 supports telecontrol event reporting and time-tagged information. Security event logging and SOC integration depend on IEC 62351 extensions, device support, and monitoring architecture.
FR7: Resource Availability	Moderate operational availability, but limited protocol-level DoS resistance. Availability should be supplemented through segmentation, connection limits, rate limiting, monitoring, and secure fallback procedures.

Constrained Application Protocol (CoAP). CoaP is a lightweight application-layer protocol designed for resource-constrained devices and low-power, lossy networks commonly found in the Internet of Things (IoT). It follows a RESTful communication model similar to HTTP, using methods such as GET, POST, PUT, and DELETE, but operates over UDP to minimize overhead and power consumption. CoAP supports features like multicast support, asynchronous message exchanges, and built-in resource discovery, making it well suited for machine-to-machine communication. Security is typically provided through Datagram Transport Layer Security (DTLS), allowing CoAP to deliver efficient, scalable, and secure communication for embedded and IoT applications. See Table 7-7 for comparison against FR 1-7.



Table 7-7. Foundational Requirements FR1-7 - CoAP assessment.

Foundational Requirement	CoAP
FR1: Identification and Authentication	Moderate to good when DTLS, OSCORE, EDHOC, or ACE profiles are used. Plain CoAP does not authenticate endpoints by itself.
FR2: Use Control	Moderate with ACE/OAuth-style constrained authorization profiles and resource-level access control. The base protocol provides REST-style methods but not a complete authorization model by itself.
FR3: System Integrity	Good when OSCORE or DTLS is deployed: supports message integrity, authenticity, and replay protection. OSCORE is particularly useful where end-to-end object security must survive proxies.
FR4: Data Confidentiality	Good when DTLS or OSCORE is enabled. Plain CoAP over UDP provides no confidentiality. OSCORE can provide end-to-end protection even across CoAP proxies, subject to correct key management.
FR5: Restricted Data Flow	Moderate. CoAP has clear REST resources and methods, which can support filtering and gateways, but multicast discovery and proxying require careful policy design.
FR6: Timely Response to Events	Limited to moderate. CoAP supports lightweight telemetry and observe-style patterns, but security event logging and auditability are not central protocol features and depend on the implementation.
FR7: Resource Availability	Moderate. CoAP is designed for constrained devices and low overhead, but UDP operation, discovery, retransmissions, and DTLS handshakes can create DoS exposure unless rate limiting and resource bounds are enforced.

Device Language Message Specification (DLMS). DLMS/COSEM (Device Language Message Specification / Companion Specification for Energy Metering) is an international standard used for communication with electricity, gas, water, and heat meters. It defines both a standardized data model (COSEM objects) and communication services that enable interoperable, secure, and vendor-independent meter reading, configuration, and control. DLMS can operate over multiple transport layers—including serial, PLC, RF, and IP networks—and supports advanced features such as time-stamped data, event logging, remote firmware updates, and strong security mechanisms with authentication and encryption, making it a cornerstone protocol for smart metering and advanced metering infrastructure (AMI).

DLMS is the de-facto standard for smart metering in Europe; the most interesting issue from a gap perspective is that it is highly complex, hard to configure (it required a second standard just to get the configuration right, which got then merged into the main standard), and thus – while allowing for a configuration that covers most gaps – also



risks configuration and implementation errors. See Table 7-8 for comparison against FR 1-7.

Table 7-8. Foundational Requirements FR1-7 - DLMS/COSEM assessment.

Foundational Requirement	DLMS/COSEM
FR1: Identification and Authentication	Good when modern high-level security and security suites are configured. DLMS/COSEM supports entity authentication and secure associations, but weak or public associations may still exist for limited access.
FR2: Use Control	Good in principle through COSEM object access rights, client roles, and association-specific privileges. The main risk is configuration complexity and inconsistent enforcement across large metering fleets.
FR3: System Integrity	Good when authenticated ciphering is used, especially AES-GCM-based security suites with invocation counters. Implementation errors, counter handling, and key reuse remain important risks.
FR4: Data Confidentiality	Good when ciphered APDUs and modern security suites are enabled. Confidentiality is optional and depends on meter configuration, key management, and whether transport layers add further protection.
FR5: Restricted Data Flow	Moderate. DLMS/COSEM has a well-defined client-server model and object structure, but flow restriction in AMI systems depends on head-end architecture, gateways, network segmentation, and meter configuration.
FR6: Timely Response to Events	Moderate to good. The protocol supports event logs, time-stamped data, and meter alarms, but security monitoring at fleet scale depends on head-end integration and consistent event collection.
FR7: Resource Availability	Moderate. DLMS/COSEM is designed for metering environments but can be complex and resource-sensitive. Availability risks include failed key rollovers, counter desynchronisation, large fleet update errors, and weak fallback procedures.

Meter-Bus (Mbus). This protocol is a European standard communication protocol designed for the remote reading of utility meters such as electricity, gas, water, and heat meters. It uses a simple master-slave architecture that allows a single master to communicate with many low-power slave devices over wired (EN 13757-2/3) or wireless (Wireless M-Bus, EN 13757-4) connections. M-Bus is optimized for long distances, low data rates, and minimal power consumption, making it well suited for battery-powered meters and building or district-level metering systems. See Table 7-9 for comparison against FR 1-7.



Table 7-9. Foundational Requirements FR1-7 - M-Bus / Wireless M-Bus assessment.

Foundational Requirement	M-Bus / Wireless M-Bus
FR1: Identification and Authentication	Limited to moderate. Wired M-Bus is often simple and physically scoped; Wireless M-Bus / OMS profiles can include device identification and security modes, but authentication depends on selected mode and implementation.
FR2: Use Control	Limited. M-Bus is primarily a metering and reading protocol and does not provide rich role-based authorization or command-level access control. Access restrictions are usually implemented by the meter, gateway, or head-end system.
FR3: System Integrity	Variable. Modern Wireless M-Bus security modes can provide authentication and integrity protection, but older or weaker modes may provide encryption only or no protection.
FR4: Data Confidentiality	Variable. Wireless M-Bus can use AES-based encryption, but security is optional and field deployments may still include unencrypted telegrams. Wired M-Bus frequently relies on physical access control and surrounding architecture.
FR5: Restricted Data Flow	Moderate in simple metering topologies. Master-slave or collector-based communication is policy-friendly, but wireless broadcast reception and multi-vendor gateways require careful key and receiver management.
FR6: Timely Response to Events	Limited. M-Bus is optimized for meter reading rather than security event response. Logging, anomaly detection, and SOC integration depend mainly on gateways and meter data management systems.
FR7: Resource Availability	Moderate for low-power metering, but limited against intentional interference, jamming, replay flooding, and battery-draining attacks. Availability protection depends on radio planning, rate limits, fallback reading, and gateway resilience.

Message Queuing Telemetry Transport (MQTT). MQTT is a lightweight, publish–subscribe messaging protocol designed for efficient communication between devices in bandwidth-constrained, high-latency, or unreliable networks. It uses a broker-based architecture where clients publish messages to topics and subscribe to topics of interest, decoupling data producers from consumers and enabling scalable, event-driven communication. MQTT runs over TCP/IP, supports different quality-of-service levels for reliable message delivery, and is widely used in IoT and smart grid applications for real-time monitoring, data aggregation, and device integration, often secured with TLS and authentication mechanisms. See Table 7-10 for comparison against FR 1-7.



Table 7-10. Foundational Requirements FR1-7 - MQTT assessment

Foundational Requirement	MQTT
FR1: Identification and Authentication	Good when broker authentication is configured using TLS client certificates, username/password over TLS, JWT, SCRAM, or equivalent mechanisms. Plain MQTT without authentication is weak.
FR2: Use Control	Moderate to good when the broker enforces topic-level ACLs, RBAC, client identity binding, and publish/subscribe restrictions. MQTT itself relies heavily on broker configuration and policy enforcement.
FR3: System Integrity	Good in transit when TLS is used. End-to-end message integrity between publishers and subscribers is not inherent because the broker terminates and redistributes messages unless application-layer signing is added.
FR4: Data Confidentiality	Good on client-broker and broker-broker links when TLS is enabled. End-to-end confidentiality between publisher and subscriber requires payload encryption or trusted broker architecture.
FR5: Restricted Data Flow	Good if topic namespaces, ACLs, broker isolation, and network segmentation are designed carefully. Poor topic design or wildcard permissions can undermine segmentation.
FR6: Timely Response to Events	Moderate to good. Brokers can log authentication failures, connection events, topic misuse, and abnormal traffic, but useful security monitoring depends on broker capabilities and SIEM integration.
FR7: Resource Availability	Moderate. MQTT supports QoS levels and resilient messaging, but brokers can become critical single points of failure and are exposed to flooding, retained-message misuse, wildcard subscriptions, and connection exhaustion unless hardened.

Narrowband Power Line Communications (NB-PLC)

- **Meters and More** is a narrowband power line communication (NB-PLC) technology used primarily for smart metering and smart grid applications, especially in Europe. It enables reliable data exchange between smart meters and utility systems over existing low-voltage power lines, supporting functions such as remote meter reading, load management, and device control. The protocol is optimized for large-scale deployments with robust performance in noisy electrical environments and is commonly used to transport higher-layer standards like DLMS/COSEM, making it a key component of advanced metering infrastructure (AMI) deployments such as those widely implemented in Italy.
- **G3-PLC** is a narrowband power line communication (NB-PLC) standard designed for smart metering and smart grid applications, enabling data



transmission over existing electrical power lines. It is optimized for low-data-rate, long-distance, and noise-prone environments, using robust modulation, adaptive tone mapping, and IPv6 support to ensure reliable communication across low- and medium-voltage networks. G3-PLC is widely adopted worldwide and commonly used to carry higher-layer protocols such as DLMS/COSEM, making it a key technology for advanced metering infrastructure and grid automation.

- **PRIME** (PowerLine Intelligent Metering Evolution) is a narrowband power line communication (NB-PLC) standard designed for smart metering and smart grid applications, enabling data transmission over existing low-voltage power lines. It supports reliable, bidirectional communication between smart meters and data concentrators using robust modulation and adaptive techniques to cope with noisy electrical environments. PRIME is widely deployed in large-scale advanced metering infrastructure (AMI) systems, particularly in Europe and parts of Asia and Latin America, and is commonly used to transport higher-layer protocols such as DLMS/COSEM for meter data management and remote utility operations. See Table 7-11 for comparison against FR 1-7.

Table 7-11. Foundational Requirements FR1-7 - NB-PLC assessment.

Foundational Requirement	NB-PLC
FR1: Identification and Authentication	Moderate. G3-PLC, PRIME, and related NB-PLC systems can support bearer security features, but endpoint identity and application authentication often depend on the carried protocol, such as DLMS/COSEM.
FR2: Use Control	Limited at the PLC bearer layer. Authorization of meter reads, commands, firmware updates, and administrative actions must normally be enforced by DLMS/COSEM, the data concentrator, or the head-end system.
FR3: System Integrity	Moderate. Some NB-PLC stacks include authentication and integrity mechanisms, but integrity for application commands and meter data should be provided by higher-layer protocols and key management.
FR4: Data Confidentiality	Moderate. Encryption may be available at the PLC or application layer, but confidentiality depends on selected profiles, key provisioning, and whether higher-layer protocols such as DLMS/COSEM are secured.
FR5: Restricted Data Flow	Moderate. PLC mesh or tree topologies support concentrator-based segmentation, but the shared physical medium, relaying, and large-scale AMI topology require careful routing, gateway, and key-domain design.
FR6: Timely Response to Events	Limited to moderate. NB-PLC can carry meter and network events, but security analytics depend mainly on concentrators, head-end systems, and fleet monitoring rather than on the PLC bearer itself.
FR7: Resource Availability	Moderate. NB-PLC is designed for noisy powerline environments and large smart-metering deployments, but availability can be affected by interference,



Foundational Requirement	NB-PLC
	topology changes, jamming, routing instability, and large-scale key or firmware update failures.

OPC UA (Open Platform Communications Unified Architecture). OPC UA is a modern, platform independent OT communications standard. OPC UA does provide native security capabilities, though these depend heavily on correct configuration. Insecure modes, anonymous access, weak certificate lifecycle management, exposed discovery services, overly broad namespace permissions, and insufficient resource limits can undermine the intended protection. OPC UA should therefore be deployed with secure profiles, certificate governance, explicit role and permission design, endpoint hardening, and monitoring integration.

As TLS, OPC UA has some level of algorithm agility build in, and thus allows to update cryptographic protocols without major disruptions, and in this does provide an important building block for future-proneness, especially with regards to quantum security See Table 7-12 Table 7-2 for comparison against FR 1-7.

Table 7-12. Foundational Requirements FR1-7 - OPC-UA assessment.

Foundational Requirement	OPC-UA
FR1: Identification and Authentication	Good when security is enabled. OPC-UA supports application authentication using certificates and user authentication using username/password, X.509 certificates, JWT, and related token mechanisms.
FR2: Use Control	Good. OPC-UA supports authorization, roles, permissions, node-level access restrictions, and separation of application and user identity. Misconfiguration or use of anonymous access can significantly weaken this capability.
FR3: System Integrity	Good. Secure channels and security policies provide signing, integrity protection, message sequencing, and replay resistance. Integrity depends on using current security policies and disabling weak or obsolete modes.
FR4: Data Confidentiality	Good when SignAndEncrypt or equivalent secure modes are used. Confidentiality is lost if SecurityPolicy None or sign-only modes are used for sensitive traffic.
FR5: Restricted Data Flow	Moderate to good. OPC-UA has explicit endpoints, services, namespaces, and access control that can support segmentation and gateways, but discovery services, aggregating servers, and PubSub architectures need careful zoning.
FR6: Timely Response to Events	Good. OPC-UA includes auditability, events, alarms, and rich metadata that can support monitoring. Effective security operations depend on enabling audit events and integrating them with monitoring and SOC tooling.



Foundational Requirement	OPC-UA
FR7: Resource Availability	Moderate. OPC-UA includes robust session and secure-channel concepts, but complex services, subscriptions, discovery, and certificate processing can be abused for resource exhaustion unless limits, rate controls, and hardening are applied.



ANNEX VI Foundational Requirements (FR1-7)

FR1 — Identification & Authentication Control (IAC). A protocol SHOULD provide:

- **Strong endpoint identity** (unique, non-spoofable identities for devices/services/users/processes).
- **Mutual authentication** (client↔server / device↔device), not just one-way.
- **Credential agility**: support for certificates/PKI, PSKs (where appropriate), and secure token-based schemes.
- **Secure bootstrap/provisioning** (initial trust establishment that resists impersonation and MITM).
- **Anti-replay of authentication** (challenge–response, nonces, channel binding).
- **No “implicit trust” modes by default** (secure-by-default posture, explicit opt-in for weaker modes).

FR2 — Use Control (UC). A protocol SHOULD provide:

- **Per-request/per-command authorization hooks** (so a receiver can enforce “who may do what”).
- **Least-privilege support** (scopes/roles/claims; separation of read vs write vs admin operations).
- **Command/operation whitelisting** (ability to disable unused/dangerous functions).
- **Session binding** (authorization bound to the authenticated identity and to the session/channel).
- **Secure delegation** (if proxies/gateways act on behalf of others, delegation must be explicit and auditable).
- **Fail-safe defaults** (deny by default on authZ failure/unknown operation).

(These map to UC as a foundational requirement.)

FR3 — System Integrity (SI). A protocol SHOULD provide:

- **Cryptographic message integrity** (MAC/AEAD) for *all* security-relevant traffic.
- **Sender authenticity** (integrity mechanism tied to the authenticated identity).
- **Replay protection** (sequence numbers, anti-replay windows, freshness guarantees).
- **Downgrade/stripping protection** (secure capability negotiation; prevent “fall back to insecure”).
- **Robust parsing & state-machine hardening** (length checks, canonicalization rules, input validation guidance).
- **Secure error handling** (no info leaks that aid attacks; consistent failure behavior).
- **Software/firmware command integrity support** (if the protocol carries updates/recipes/config, support signing & verification semantics).

(These map to SI as a foundational requirement.)



FR4 — Data Confidentiality (DC). A protocol SHOULD provide:

- **Encryption in transit** for sensitive data and credentials.
- **Modern cipher suites** with **perfect forward secrecy (PFS)** where feasible.
- **Protection of credentials and secrets** (no plaintext passwords/keys; no weak challenge/response).
- **Optional payload confidentiality end-to-end** (useful where intermediaries exist).
- **Traffic analysis minimization where needed** (limit sensitive metadata exposure; padding if warranted by threat model).

(These map to DC as a foundational requirement.)

FR5 — Restricted Data Flow (RDF). A protocol SHOULD make it *possible* to enforce zoning/conduits and segmentation by:

- **Deterministic, policy-friendly communications** (well-known ports, minimal protocol surface).
- **Explicit endpoint and service identification** (so firewalls/allow-lists can be precise).
- **Support for gateway/proxy patterns** (secure traversal between zones without flattening segmentation).
- **No unnecessary broadcast/multicast** (or make it disable-able).
- **Granular routing/control-plane separation** (don't mix discovery, admin, and control traffic unless separable).
- **Compatibility with filtering/inspection** (clear message framing; ability to block classes of operations).

(These map to RDF as a foundational requirement.)

FR6 — Timely Response to Events (TRE). A protocol SHOULD support detection/response workflows by providing:

- **Security event generation** semantics (auth failures, replay detects, policy violations, integrity failures).
- **Audit-relevant metadata** (who/what explained by identity, operation, target, timestamp, result).
- **Clock/time synchronization assumptions explicitly stated** (and safe behavior when time is wrong).
- **Session termination & revocation responsiveness** (ability to drop sessions on revoke; short-lived tokens; re-auth triggers).
- **Alarm/telemetry channel protection** (events should be integrity-protected; confidentiality as needed).

(These map to TRE as a foundational requirement.)

FR7 — Resource Availability (RA). A protocol SHOULD be resilient against misuse and DoS by design:

- **Bounded resource consumption** (strict limits on message sizes, nesting, decompression, fragmentation, retries).
- **Rate limiting guidance** (per peer / per identity / per operation).



- **Handshake DoS protections** (stateless cookies, puzzles, or other amplification resistance).
- **Timeouts and backoff** (avoid lockups and retry storms).
- **Priority/QoS support** where applicable (control traffic vs bulk/diagnostics).
- **Graceful degradation** (continue safe operations under partial failure, reject expensive features first).
- **No easy amplification vectors** (reflection, broadcast replies, unauthenticated heavy responses).

(These map to RA as a foundational requirement.)

